HP SureStore NetStorage 6000

User's Guide

© 2000 - 2001 Hewlett-Packard Company.

The information contained in this document is subject to change without notice.

This document contains proprietary information which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of Hewlett-Packard Company.

Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages (including lost profits) in connection with the furnishing, performance, or use of this material whether based on warranty, contract, or other legal theory.

Part Number C4475-90102

Table of Contents

Chapter 1: Overview

Network Attached Storage 1-1
Getting Started. 1-1
HP NetStorage 6000 Hardware 1-3
The HP NetStorage 6000 Web Interface 1-9
Integrating with Network Management Applications. 1-11
Backing up the HP NetStorage 6000. 1-12
Locating Information 1-13
Using Help While You Work 1-14
Printing Documents. 1-14

Chapter 2: The Identity Tab

Chapter 3: Configuring Your System and Network

The Configuration Tab 3-1
Network Settings. 3-2
Alert Settings. 3-7
System Settings 3-10
User Mapping 3-14
Shutting Down and Restarting 3-21

Chapter 4: Managing Storage

The Storage Tab 4-1
Managing Physical and Logical Drives 4-2
Managing File Volumes and Directories. 4-8
Allowing Access to Data. 4-14

Chapter 5: Backing Up and Restoring Files

The Backup and Restore Tab 5-1
Using the HP SureStore 818 or 1/9 DLT Autoloader 5-1
Local and Remote Backups. 5-4
Disk Checkpoints 5-7
Checking the Current Tape Drive Status. 5-11
Backing Up 5-14
Restoring Volumes, Files, and Directories 5-18
Checking Settings and Features 5-21

Chapter 6: Monitoring the System

The Status Tab. 6-1
Monitoring Hardware Information 6-1
Viewing System Activity 6-6

Chapter 7: Reporting

The Report Tab 7-1

Chapter 8: Securing Data

About HP NetStorage 6000 Security 8-1
HP NetStorage 6000 Security in a UNIX-only Environment 8-1
HP NetStorage 6000 Security in an NT-only Environment 8-4
Security Mapping in a Heterogeneous Environment 8-9
UNIX Files Accessed by NT Clients 8-10
NT Files Accessed by UNIX Clients 8-11
Mapping NT and UNIX Users 8-12
Modifying Map Files. 8-13

Chapter 9: Contacting Support and Upgrading

The Support Tab 9-1
Upgrading the HP NetStorage 6000 9-3

Chapter 10: Integrating with Management Applications
Management Applications Overview 10-1
HP Top Tools Integration 10-3
HP OpenView Network Node Manager Integration 10-4
CA Unicenter TNG Framework Integration 10-7
ManageX Integration 10-10

Chapter 11: Integrating with Remote Backup Applications
Remote Backup Applications Overview 11-1
Using ARCserveIT 11-2
Using Backup Exec 11-4
Using HP OpenView OmniBack II 11-5

Appendix A: Legal Information
Statements A-1
Software License Agreement A-2

Appendix B: NetStorage 6000 Warranty Information
Planning for Support B-1
Obtaining Warranty Support B-3
Obtaining Out-of-Warranty Support B-5
Hewlett-Packard Limited Warranty Statement B-6

Appendix C: System Specifications
Central Processing Unit (CPU) C-1
Uninterruptible Power Supply (UPS) C-2
Hardware Specifications C-3
Features C-5
Upgrade Options C-6
Security and Safety C-6
Regulatory Compliance C-7
Environmental Specifications C-8
Power Specifications C-10
Replacements and Upgrades C-11

Appendix D: Telnet Information

Appendix E: Troubleshooting and Error Codes

General Issues E-1
Browser Issues E-4
Determining Component Failure. E-6
UPS Troubleshooting E-8
Hardware Error Codes. E-10

Glossary

Chapter 1
Overview

Network Attached Storage

The HP NetStorage 6000 is a network attached storage (NAS) device used to store data on your network. NAS devices provide a simpler, more reliable, and cost-effective way to add storage to your network.

The HP NetStorage 6000:

- Requires minimal setup and is easily maintained
- Does not impact the productivity of existing general-purpose server operations
- Frees up the general-purpose server so that applications operate more efficiently
- Contains SCSI hard drives in a pre-configured RAID 5 array
- Provides SNMP notification of critical events
- Provides SMTP/E-mail for critical evens

Getting Started

Before proceeding, make sure that you have installed and configured the HP NetStorage 6000 device by entering the IP, gateway, subnet, and broadcast addresses via the front panel of the HP NetStorage 6000. For more information, refer to *Installing the HP NetStorage 6000*.

Once the front panel information has been entered, you must use the HP NetStorage web interface to finish configuring your device:

1. Open the HP NetStorage web interface. (Once the web interface is open, you can access help online.) See “The HP NetStorage 6000 Web Interface” on page 1-9.

2 Go directly to the Configuration Tab and manually enter:

- System name, see “DNS Settings” on page 3-3
- Administrative password, see “Administrative Password Settings” on page 3-12
- DNS domain name, see “DNS Settings” on page 3-3
- Primary and secondary DNS server IP addresses, see “DNS Settings” on page 3-3
- NIC parameters, see “TCP/IP Settings” on page 3-2
- Address for event log data, see “System Log” on page 3-9
- UNIX settings, see “UNIX Settings” on page 3-4
- WINS settings, see “Windows Settings” on page 3-6
- SMTP server information, see “SMTP/Email” on page 3-7
- SNMP settings/Traps, see “SNMP/Network Management Settings” on page 3-8
- Contact and asset information, see “Informational Settings” on page 3-10
- System time and date, see “Date and Time Settings” on page 3-11
- User mapping information, see “Mapping Strategy” on page 3-14

3 Go to the Storage Tab and manually:

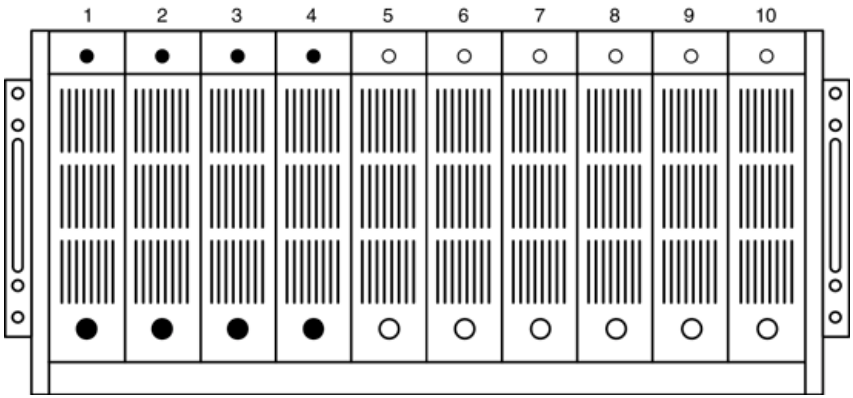
- Group your physical drives into logical drives (RAID sets) if required, see “Create a Logical Drive” on page 4-4
- Create volumes for data storage, see “Create a New File Volume” on page 4-9
- Create directories and sub-directories beneath your volumes, see “Create a Directory” on page 4-12
- Make volumes or directories available to users by sharing or exporting them, see “Create or Edit Windows Shares” on page 4-14

HP NetStorage 6000 Hardware

Physical Drives

The HP NetStorage 6000 contains between four and ten physical hard drives, depending on your company's storage needs. Each physical drive can have up to 73GB of storage capacity.

Figure 1.1 Physical Drives



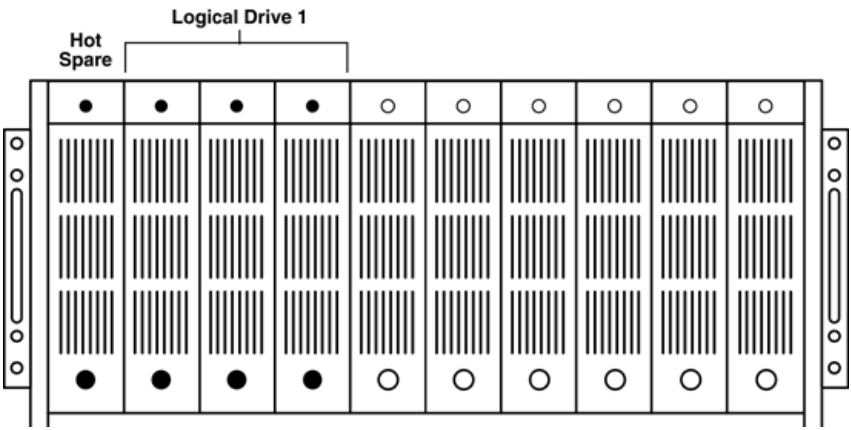
Note	Use only HP Hard Drives approved for your NetStorage 6000. For an up-to-date list of approved hard disk drives, please visit our web site at www.hp.com/support/ns6000. Drives on the approved list have custom firmware for use in your NetStorage 6000. Do not attempt to install any hard disk drives other than the approved drives listed at this web site as doing so may result in system failure or loss of data. Using non-supported hard drives may also void your warranty.

Note	All drives in the HP NetStorage 6000 must have the same capacity. **Any other configuration is not supported.**

Logical Drives

Physical drives are grouped together to form one or more logical drives, which are also known as RAID sets. Physical drives are also used individually as hot spares. Logical drives and hot spares are configured at the factory. The illustration in figure 1.2 shows a typical configuration.

Figure 1.2 Logical Drives



Note The HP NetStorage 6000 supports only RAID level 5 for the creation of logical drives. Because RAID level 5 requires a minimum of 3 physical drives for a RAID set, the HP NetStorage 6000 requires at least 3 drives to be grouped together to create a logical drive, though you can create a logical drive that uses as many as eight physical drives.

Partitions and File Volumes

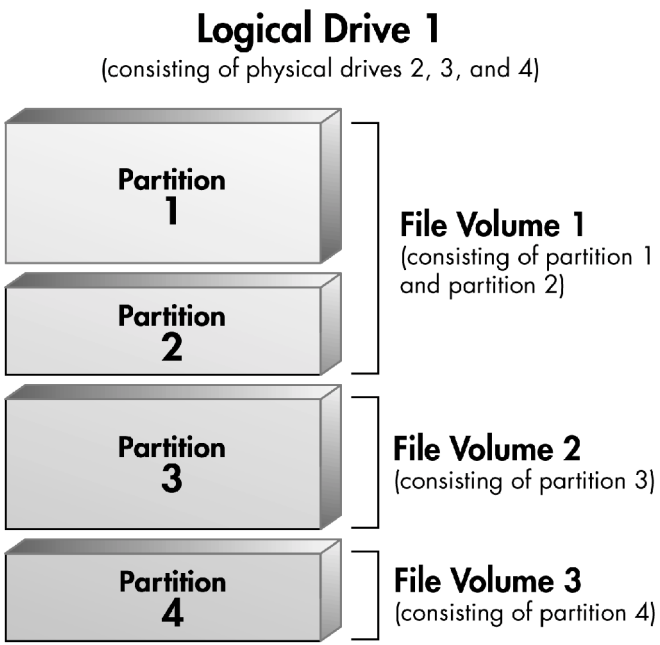
Logical drives are further broken down into as many as four partitions with each partition consisting of 256GB of drive space or less. Once you have partitioned your logical drive, you can create file volumes for storing your data.

File volumes are the basic unit of logical storage for a file system on the HP NetStorage 6000. When you create a file volume, it uses one partition on one logical drive. Because you are limited to four partitions, the maximum number of file volumes that can be created on a logical drive is four.

Note	The HP NetStorage 6000 has a limit of 256GB (262144 MB) per partition. The user interface does not warn you of this limitation. If you attempt to create a partition greater than 256GB, the operation fails.

Initially, each partition is assigned to a file volume. However, file volumes can expand to span several partitions if extra storage space becomes necessary.

Figure 1.3 File Volume and Partition Example



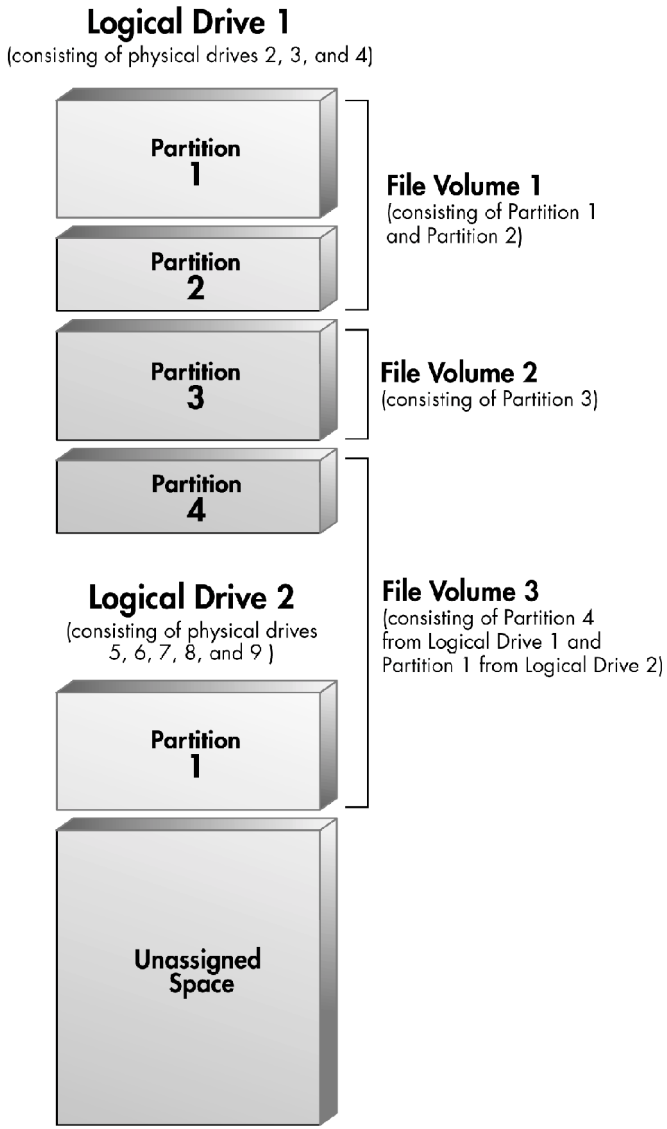
The illustration in figure 1.3 on page 1-5 shows a logical drive that consists of three physical drives. This logical drive has been broken down into four partitions (the maximum number). Typically, you create partitions such that each one becomes a file volume. However, at some point you may require more storage space for a file volume.

Increasing Storage Capacity

An important aspect of managing file volumes is the concept of expanding volumes. If, at a later date, a file volume becomes full of data, you can *expand* the file volume, thus alleviating the lack of space on the volume. Just like creating new file volumes, expanding file volumes need storage space from a logical drive, and a free partition. However, this free space and free partition do not have to be on the same logical drive as the file volume that is being expanded. Thus, it is possible to create file volumes that span across logical drives. This gives you the option of expanding existing volumes by installing another logical drive on the system.

The example shown in figure 1.4 on page 1-7 expands on the previous example by adding a new logical drive consisting of five newly added physical drives. This logical drive has had one partition defined. File volume 3 has then been expanded to include this newly available space.

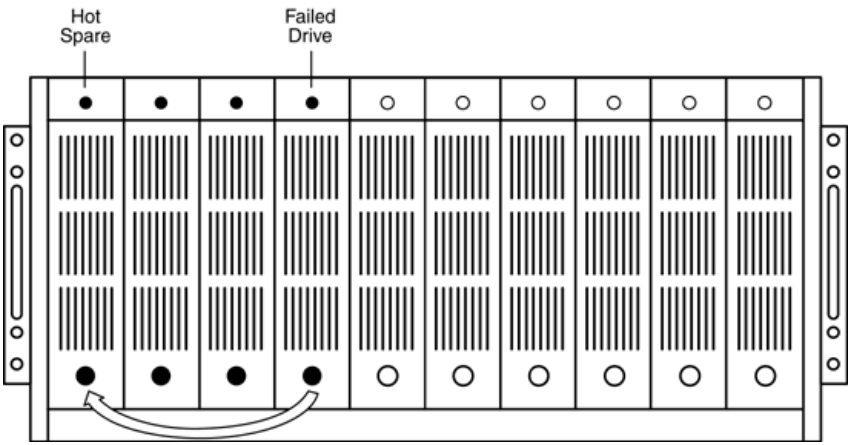
Figure 1.4 Expanding File Volumes


Logical Drive 1
(consisting of physical drives 2, 3, and 4)
Partition 1
Partition 2
Partition 3
Partition 4
File Volume 1
(consisting of Partition 1 and Partition 2)
File Volume 2
(consisting of Partition 3)
File Volume 3
(consisting of Partition 4 from Logical Drive 1 and Partition 1 from Logical Drive 2)
Logical Drive 2
(consisting of physical drives 5, 6, 7, 8, and 9)
Partition 1
Unassigned Space

Hot Spare Drives

Hot spare drives are reserved drives that are used only when a physical drive that is part of a logical drive fails. When this happens, the system automatically selects the first available hot spare drive to take the place of the failed drive as shown in figure 1.5. The logical drive is rebuilt using the hot spare, and the hot spare drive becomes a member of the logical drive.

Figure 1.5 Hot Spare Drive



It is important to note that a hot spare must have the same or larger capacity of the physical drive it is to replace. The system will not select a hot spare to replace a failed drive if the capacity of the hot spare is less than the drive it is to replace.

Once a hot spare is used to repair a logical drive, its assignment changes from Hot Spare to Online. If you replace the failed drive, it automatically receives an assignment of Unassigned. You must manually assign the new drive to Hot Spare if the new drive is to serve as a hot spare.

Redundant Power Supply Modules

A redundant power supply module is installed in the back of the HP NetStorage 6000. Three power-supply modules are active but only two are necessary to power a fully loaded unit. If a power supply module fails, the redundant supply provides power to the unit.

Redundant Power Supply Cords

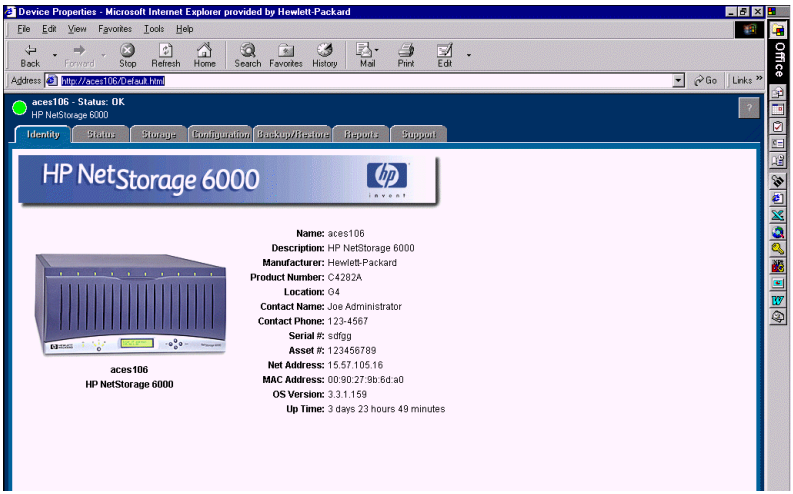
The HP NetStorage 6000 lets you attach more than one power source into the back of the unit. This redundancy protects against a power failure. The primary power cord needs to be connected when power is turned on.

The HP NetStorage 6000 Web Interface

The HP NetStorage 6000 is managed via a web browser as shown in figure 1.6 on page 1-10 (Internet Explorer 5.0 or later or Netscape 4.61 or later). To access the web interface, enter the IP address of the HP NetStorage 6000 in the address field of your browser.

Note The first time you open this interface, a security warning appears. The NetStorage web interface uses Java and Javascript components to properly display system information. Your browser detects that such programs are running and asks for your permission to accept these software components. You must accept content from or grant privileges to Hewlett-Packard Company. To prevent further security warnings from appearing, check the box at the bottom of the window to always trust content from Hewlett-Packard Company.

Figure 1.6 HP NetStorage 6000 Web Interface



The web interface's six tabs are:

- **Identity Tab** — View general system information. See Chapter 2, "The Identity Tab."
- **Status Tab** — View system activity and monitor hardware information. See Chapter 6, "Monitoring the System."
- **Storage Tab** — Create and delete file volumes and directories; create shares and mount points; modify permissions; view file volume information; view physical drive specifications. See Chapter 4, "Managing Storage."
- **Configuration Tab** — Initialize, view, and modify network, alert, and system settings for your device. See Chapter 3, "Configuring Your System and Network."
- **Backup/Restore Tab** — Check the current tape drive status; create disk checkpoints; schedule a backup; restore volumes, files, and directories; check settings and features. See Chapter 5, "Backing Up and Restoring Files."
- **Support Tab** — Request information about the HP NetStorage 6000, and register and upgrade your operating system. See Chapter 9, "Contacting Support and Upgrading."
- **Reports Tab** — Provides information on hardware and software, file system configuration, NIC configuration, and environmental status to up to three email addresses.

Integrating with Network Management Applications

Network management applications let you view and manage devices on your network. The HP NetStorage 6000 works with the following management applications:

- HP TopTools versions 4.5 and 5.0
- HP OpenView Network Node Manager version 6.0
- Computer Associates Unicenter TNG Framework version 2.2
- HP OpenView ManageX version 4.21

The integration lets each network management application:

- Identify the HP NetStorage 6000 when it is attached to the network
- Display the HP NetStorage 6000 icon in the platform's network topology map
- Launch the HP NetStorage 6000 web-based user interface from a pop-up menu
- Receive and process event notifications from the HP NetStorage 6000

For more information, see Chapter 10, "Integrating with Management Applications."

Backing up the HP NetStorage 6000

Local Backup

You can use the backup application in the NetStorage web interface plus an optional HP SureStore DLT Autoloader 818 or 1/9 to perform a local backup. In a local backup session the data is transferred to the locally attached Autoloader using a tape format that is unique to the HP NetStorage 6000. The data transfer does not interfere with your LAN traffic.

Remote Backup

You can use third-party backup applications on any computer on the network with a tape drive attached to perform a remote backup. When you run a remote backup, data from the HP NetStorage 6000 transfers over the network to the remote server running the backup application, and then to the server-attached tape device.

Tape backup is intended to replace the data of an entire drive. It is possible to restore individual files, but only if you know the exact location of a file.

For a list of remote backup applications the HP NetStorage 6000 integrates with, see Chapter 11, “Integrating with Remote Backup Applications.”

Locating Information

The online User's Guide works with HP TopTools version 5.0. If you do not have TopTools on your system, you can use a web browser to view the user's guide (Internet Explorer 5.0 or later or Netscape 4.61 or later). The context-sensitive, online User's Guide is pre-loaded on your HP NetStorage 6000.

The guide is organized into main level and sub-level topics.

The left-hand tabs in this help system are:

- **Contents** — The Contents tab displays folders and pages that represent the categories of information in the online user's guide. When you click a closed folder, it opens to display its content (subfolders and pages). When you click an open folder, it closes. When you click pages, you select topics to view in the right-hand pane.
- **Index** — The Index tab displays a list of keywords and keyword phrases. These terms are associated with topics in the help system. To open a topic in the right-hand pane associated with a keyword, double-click the keyword.

A PDF version of the user's guide is also located on the HP NetStorage 6000 CD.

Note Viewing the PDF-format *HP SureStore NetStorage 6000 User's Guide* requires Adobe Acrobat Reader.

To view this version:

1. Insert the HP NetStorage 6000 CD into your CD-ROM drive.
2. Open a **Windows Explorer** window.
3. Click on your CD-ROM drive and locate the directory **/Doc**.
4. Double-click on the file `UserGuid.pdf` to view it.

Using Help While You Work

You can obtain information about the tabs in the NetStorage web interface by using context-sensitive help.

1. Click the **help** icon in the upper right corner of the web interface window. A help window displays the topic pertaining to the screen you are viewing.
2. Review the information, then close the window, or leave help running in the background by minimizing the screen.

When viewing help, you can maximize the window or resize it with the buttons in the upper-right corner.

Note Clicking the **help** icon in the upper right corner does not automatically bring the on-line help browser window to the top; it may be hidden by another window. You must raise the window manually by clicking in the window, clicking the title bar of the window, or selecting it from a task list

Printing Documents

While using the online user's guide, you can print topics and information directly from the viewer. The available print options are determined by the version of TopTools or your browser.

Select **File > Print** and click the options you want for the screen(s) you are printing.

Chapter 2
The Identity Tab

The Identity tab displays the following general system information:

- **Name—**The system or host name for your HP NetStorage 6000
- **Description—**HP NetStorage 6000
- **Manufacturer—**Hewlett-Packard Company
- **Product Name—**The product number corresponding to the original configuration of the HP NetStorage 6000
- **Location—**The physical location of the HP NetStorage 6000
- **Contact Name—**The person to be notified in case of trouble or questions about the HP NetStorage 6000 (usually the system administrator)
- **Contact Phone—**Usually the phone number of the contact name
- **Serial #—**The factory-set serial number of the unit
- **Asset #—**A user-assigned number to track company assets
- **Net Address—**The IP network address of the Network Interface Card (NIC) in port 1 (although the HP NetStorage 6000 supports multiple ports, only the first one is displayed)
- **MAC Address—**The unique Machine Address Code for the NIC in port 1
- **OS Version—**The current version of the operating system running on the HP NetStorage 6000
- **Up Time—**The cumulative up-time of the HP NetStorage 6000 since the last reboot

You can change the Name, Location, Contact Name, Contact Phone and Asset # using the NetStorage 6000 web interface. See“Informational Settings” on page 3-10 for more information.

Chapter 3
Configuring Your System and Network

The Configuration Tab

When you initially set up your HP NetStorage 6000, you must:

- Enter your TCP/IP settings.
- Configure your Network Interface Card parameters.
- Set up your UNIX and/or Windows environments.

If your network configuration changes, you need to alter these settings.

The Configuration tab lets you access:

- **Network settings** — TCP/IP, Windows and UNIX settings that allow the NetStorage 6000 to connect with your network and work in Windows, UNIX or both operating systems.
- **Alert settings** — Optional settings you can enter if you want to receive e-mail or server notification in case of a hardware failure or system alerts. You also can specify a remote server to which you can redirect a copy of the event log.
- **System settings** — Optional informational settings. You can specify the date and time as well as password-protect the administration of your NetStorage web interface.
- **User mapping** — Configuration and management tools for operating the HP NetStorage 6000 in a heterogeneous environment with user-level security for NT clients.
- **Shutdown/Restart** — You can shut down or restart the HP NetStorage device from the Configuration tab.

Network Settings

TCP/IP Settings

The HP NetStorage 6000 has two Network Interface Card (NIC) slots and supports the following NICs:

- Single-port 10/100 Base-T
- Dual-port 10/100 Base-T
- Gigabit 1000 Base SX

This support gives the system between one and four NIC ports. When you initially set up your HP NetStorage 6000, you need to configure your IP address for the NIC using the front panel display. If you have Dynamic Host Configuration Protocol (DHCP) on your system and it is enabled, NIC configuration occurs automatically.

If you add a new card or change your IP address, you need to reconfigure the NIC parameters by filling in each of the individual fields on the **TCP/IP Settings** screen.

To set the NIC parameters:

1. Select one of the following two options:
   - **Obtain an IP address from the DHCP Server** sets the parameters automatically if DHCP is enabled. Because the parameters are under DHCP control, you can not enter or change the IP Address or subnet mask. If you disable DHCP and then later decide to enable it, you will need to restart your device.
   - Depending on your configuration, the DHCP server provides any or all of the following parameters: System Name, Gateway IP Address, DNS Domain Name, NIS parameters, and Windows parameters. You must manually configure any parameter that DHCP does not set. You need to reboot your system to configure the DHCP parameters.
2. **Specify an IP Address** lets you enter the IP Address and subnet mask. The text fields show the current value which can be changed by entering a static IP Address and/or subnet mask. (If you do not have optional NIC ports, **Not Installed** displays beneath the NIC port fields.)

3 Click **Apply**. A dialog box informs you that:

- You are about to change the system's NIC parameters. You (and other users) will lose the connection to the device while the changes take place.
- The NetStorage web interface in the current browser cache becomes invalid. You should close the browser and reconnect to the system using the new NIC parameters.
- Any invalid entries in the NIC parameters may result in an inability to access the NetStorage web interface.

4 Click **OK**. You do not need to restart the system.

NIC parameter fields are provided for up to three optional NIC ports. They behave identically to the fields for the primary NIC.

DNS Settings

To define the DNS settings:

1 Using the NetStorage web interface, click the **Configuration** tab, then select **Network Settings > DNS Settings**.

2 Enter the:

- System Name (Host or Computer Name)
- DNS Domain Name (Name of the domain on which the HP NetStorage 6000 device resides such as, alpha.corp.com)
- Primary and Secondary DNS server IP addresses

3 Click **Apply**. You do not need to restart the system.

UNIX Settings

During initial setup, you must specify how to manage and maintain the Hosts and Trusted Hosts files. Hosts file management lets you map a machine name to its IP address. Trusted Hosts file management lets you configure hosts on your network so that they have a *trusted* relationship with the HP NetStorage 6000. A *trusted* relationship lets the host perform administrative functions, such as file changes and remote network backup (on the HP NetStorage 6000).

To add a Hosts file:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Network Settings > UNIX Settings**.
2. Click **Add** next to the **Hosts File Management** field. The **Add Host File Entry** screen appears.
3. Enter a **Host Name** and a **Host IP Address**.
4. If you are adding:
   - multiple hosts, you need to click **Apply** after each addition, then click **OK** when you finish.
   - only one host, you can simply click **OK**.

To modify or delete an existing Hosts file:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Network Settings > UNIX Settings**.
2. Select a host from the **Hosts** drop-down list.
3. Click either:
   - **Edit**. Modify the **Host Name** and **Host IP Address**, then click **Apply**.
   - **Remove**. Click **OK** to confirm your selection.

To set up a Trusted Host, you must first specify it in the Hosts file:

Note	Making a host trusted may compromise network security and should only be done for administrative purposes.

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Network Settings > UNIX Settings**.
2. Click **Add** next to the **Trusted Hosts File Management** field. The **Add Trusted Host Entry** screen appears.
3. Enter the host name.
4. If you are adding:
   - multiple trusted hosts, you need to click **Apply** after each addition, then click **OK** when you finish.
   - only one trusted host, you can simply click **OK**.

To change or delete an existing trusted host:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Network Settings > UNIX Settings**.
2. Select a host from the **Hosts** drop-down list.
3. Click either:
   - **Edit**. Modify the **Trusted Host Name**, then click **Apply**.
   - **Remove**. Click **OK** to confirm your selection.

Windows Settings

If you support Windows users, you must specify the Windows settings during initial setup.

To specify the Windows settings:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Network Settings** > **Windows Settings**.
2. Enter the:
   - **Primary** and **Secondary WINS IP Addresses**
   - **Network Neighborhood System Comment** (optional)
3. Click either **User Level Security** or **Share Level Security** for the security mode. See “User-Level Security” on page 8-6 or “Share-Level Security” on page 8-5 for more information.
   a. If you select **User Level Security**, enter the:
      — **Domain Name**
      — **Domain Login Name** (the login name specified must have sufficient permission to allow machines to be added to the domain)
      — **Domain Password**
   b. If you select **Share Level Security**, enter the name of the **Workgroup** where the HP NetStorage 6000 is a member.
4. Click **Apply**. You do not need to restart the system unless you changed your security mode.

Alert Settings

SMTP/Email

The HP NetStorage 6000 lets you automatically notify individuals via e-mail if there is a hardware failure or a critical system alert.

To set up automatic notification:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Alert Settings > SMTP/email**.
2. Enter the name of the e-mail server. The e-mail server must be an IP address or a fully qualified name (such as, alpha.corp.com).

Note If you change the e-mail server, it automatically changes the e-mail server specified in the Reports tab. See “The Report Tab” on page 7-1.

3. Enter the e-mail addresses of as many as four individuals. You must specify an e-mail server if one or more e-mail recipients are defined.
4. Click either:
   - **Send Test email** to send a test message to the recipients and save your settings.
   - **Apply** to only save your settings.

Note The information on this screen is optional. Blank fields do not affect the functionality of the device. In the event of a hardware failure or system alert, messages are sent through the network management tool or they are logged in the event log. See “View Event Log” on page 6-3.

SNMP/Network Management Settings

If you are using a Simple Network Management Protocol (SNMP) tool, you can define the names of the servers to receive notification in case of a failure.

To define the servers to receive notification:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Alert Settings > SNMP/Network Management**.
   By default, the **Community String** field is set to `public` and the **Trap Destination** fields are blank.
2. In the **Trap Destination** fields, enter the IP addresses or names of the servers you want the system to notify (up to five).
3. Enter a value in the **Volume Capacity Threshold** field to receive a warning message if your volume gets to a certain capacity. By default, the field is set to 95 percent
4. Click either:
   - **Send SNMP Test Trap** to send a cold boot test trap to the destination addresses and save your changes.
   - **Apply** to only save your settings.

Note	The information on this screen is optional. Blank fields do not affect the functionality of the device.

System Log

You can define a remote server to which you can redirect a copy of the event log. For more information, see “View Event Log” on page 6-3. The **Syslog** function lets you manage a central location for the event log instead of working with different interfaces or systems. The **Syslog** function allows the event log to be redirected to systems with a Syslog daemon.

Note Red Hat Linux 6.1 requires that you set the -r option in the syslog daemon to enable the device to receive messages from the network. This action, along with defining the remote server on the SYSLOG page, allows the HP NetStorage 6000 event log messages to appear in the Red Hat Linux 6.1 system log file.

To define a remote server to receive a copy of the event log:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Alert Settings > Syslog**.
2. Enter the name or IP address of a remote server to redirect the event log to. (If the field blank, this feature is disabled.)
3. Click **Apply**.

Note System log information is optional. A blank field does not affect the functionality of the device.

System Settings

Informational Settings

The **Informational Settings** appear on the **Identity** screen of the NetStorage web interface. Network management tools may also function according to the contents of these fields.

To change the informational settings:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **System Settings > Informational Settings**.
2. Enter the:
   - Name of the person primarily responsible for the HP NetStorage 6000 in the **Contact Name** field.
   - Phone number of the person primarily responsible for the HP NetStorage 6000 in the **Contact Phone Number** field.
   - Description of the physical location of the HP NetStorage 6000 in the **System Location** field.
   - Number that your company might use to identify and track the HP NetStorage 6000 in the **Asset Number** field.
3. Click **Apply**.

Note Blank fields do not affect the functionality of the device. However, entering your system location lets you easily determine which device has issued an alert when you receive notification of an error. (The e-mail message contains the system name.) If you provide your system location information, you can easily troubleshoot or repair the problem.

Date and Time Settings

Although not required, you should set the date and time on the HP NetStorage 6000. The system uses the information on this screen to keep track of the date and time for operations such as:

- Backup
- Time stamps for file generation and modification
- Log file reports

Failure to set the proper date and time may lead to confusing behavior or misleading time stamping of files and log messages.

To set the date and time:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **System Settings > Date and Time**.
2. Enter the:
   - current date using the format **mm/dd/yyyy**.
   - current time using military format **hh:mm**.
3. Select a **Time Zone** for your area from the pull-down menu.
4. If desired, check **Automatically Adjust Clock for Daylight Savings Changes**.
5. Click **Apply**.

Administrative Password Settings

You can set a password for the HP NetStorage 6000. This prevents unauthorized access to the storage device's web interface. The HP NetStorage 6000 ships without password protection, and the fields are initially blank.

Note If you set a password for the HP NetStorage 6000, protect it as you would any other password. If you forget or lose this password, you will not be able to access your device. Call HP Support for assistance. See "HP NetStorage 6000 Service and Support" on page 9-1.

If you specify a password, you must know the password to view or modify the information in the other tabs. You can not access the NetStorage web interface without the password.

To initially specify a password:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **System Settings > Administrative Password**.
2. Leave the **Old Password** field blank. Enter a password in the **New Password** field. Use any combination of letters and numbers, and uppercase and lowercase characters.
3. Confirm your password by typing it again in the **Confirm New Password** field.
4. Click **Apply**.
5. A dialog box informs you that your password is set. Click **OK**.

Note If you did not correctly confirm your password, a dialog box prompts you to re-enter your password

To change your password:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Systems Settings > Administrative Password**.
2. Enter your password in the **Old Password** field.
3. Enter a new password in the **New Password** field. You can use any combination of letters and numbers, and uppercase and lowercase characters.
4. Confirm your password by typing it again in the **Confirm New Password** field.
5. Click **Apply**.
6. A dialog box informs you that your new password is set. Click **OK**.

To remove a password:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Systems Settings > Administrative Password**.
2. Enter your password in the **Old Password** field.
3. Leave the **New Password** and **Confirm New Password** fields blank.
4. Click **Apply**.
5. A dialog box informs you that your new password is set. Click **OK**.

Note A dialog box prompts you to re-enter your password if you did not type your old password, you typed an incorrect password in the **Old Password** field, or you did not correctly confirm your password.

Hardware Settings

The HP NetStorage 6000 may be attached to an uninterruptible power supply (UPS).

To enable or disable HP NetStorage 6000 support for the UPS:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **System Settings** > **Hardware Settings**.
2. Check **External power supply (UPS) attached** if you are going to attach a UPS to the HP NetStorage 6000. Clear this setting if you are going to use the HP NetStorage 6000 without a UPS.
3. Click **Apply**. In order for the changes to take effect, you need to restart your system.

Note	For a list of supported UPS devices, see Appendix , “System Specifications.”

User Mapping

Mapping Strategy

The HP NetStorage 6000 server is a general purpose file server with capabilities to serve files to Windows clients and UNIX/Linux clients using the native file serving protocol of each client. In order to allow clients to access the same files, with the same access privileges, it is necessary to map the equivalency of the UNIX and Windows accounts. The mapping occurs on both a user and Windows primary group level. In order to create this mapping or association, it is necessary to specify an overall strategy and then manage the mapping files as needed.

For more information, see “Mapping NT and UNIX Users” on page 8-12.

To select a mapping strategy:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **User Mapping > Mapping Strategy**.
2. Select a User Mapping strategy. The possible choices are:
   - **No Mapping** — No automatic mapping between UNIX NIS accounts and Windows accounts occurs. Any mapping between accounts must be done by editing the user map file for each account.
   - **User Name Mapping** — If the Windows and UNIX usernames from the NIS files are identical, then a mapping association is automatically created in the user map file.
   - **Full Name Mapping** — If the Windows full name field and the UNIX comment field in the NIS file, are identical then a mapping association is automatically created in the user map file.
3. Select a Group Mapping strategy. The possible choices are:
   - **No Mapping** — No automatic mapping between a UNIX NIS group file and Windows primary group account occurs. Any mapping between group accounts must be done by editing the group map file for each account.
   - **Group Name Mapping** — If the primary Windows group account and the UNIX NIS group account names are identical then a mapping association is automatically created in the group map file.
4. Click **Apply** when you are satisfied with your mapping choices.

NIS User Accounts

Note The HP NetStorage 6000 supports NIS service, but not NIS+ service.

The HP NetStorage 6000 allows you read-only access to portions of the user NIS file generated by the Network Information Service (NIS) when NIS is enabled. This information is provided for assistance if you find that you need to make modifications to the user map file. The user map file associates an NT or Windows user with a UNIX user account. NT or Windows client information is automatically captured by the NetStorage 6000. Depending upon the user mapping strategy that you have selected, you may find that you wish to create an association between a specific Windows or NT client and a UNIX account. In order to make this custom association you need the UNIX user name and UID. You can scroll through the user NIS file to find the UNIX account name and UID that are needed to complete the custom mapping.

Once you have identified the UNIX user name and UID value, you can modify the user map file using the NetStorage web interface. Fill in the appropriate fields with the UNIX user account information.

For more information, see “Mapping Strategy” on page 3-14 and “Modifying the User Map File” on page 3-19.

Note In order to see the user NIS file, the NIS service must first be enabled.

To enable or disable NIS (disabled is the default) for User Accounts:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **User Mapping > NIS User Accounts**.
2. Click on **NIS Service**.
3. Check or clear **Enable NIS**. If you are enabling NIS, enter the:
   - master server’s IP address in the **NIS Server** field.
   - appropriate NIS domain name in the **NIS Domain** field.
4. Click **Apply**. You do not need to restart the system.

The NIS files are automatically updated every 5 minutes when the NIS service is enabled. If the service is disabled, you see either stale data or an informational message indicating that the file is empty.

Note The NIS service can be enabled from either the NIS User Account page or the NIS Group Account page.

NIS Group Accounts

Note	The HP NetStorage 6000 supports NIS service, but not NIS+ service.

The HP NetStorage 6000 allows you read-only access to portions of the user NIS file generated by the Network Information Service (NIS) when NIS is enabled. This information is provided for assistance if you find that you need to make modifications to the group map file. The group map file associates an NT or Windows primary group with a UNIX group account. NT or Windows primary group account information is automatically captured by the NetStorage 6000. Depending upon the group mapping strategy that you have selected, you may find that you wish to create an association between a specific Windows or NT client and a UNIX account. In order to make this custom association, you need the group name and GID. You can scroll through the group NIS file and find the UNIX group name and GID that are needed to complete the custom mapping.

Once you have identified the UNIX group name and GID value, you can modify the group map file using the NetStorage web interface. Fill in the appropriate fields with the UNIX group account information.

For more information, see “Mapping Strategy” on page 3-14 and “Modifying the Group Map File” on page 3-20.

Note	In order to see the group NIS file, the NIS service must first be enabled.

To enable or disable NIS (disabled is the default) for Group Accounts:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **User Mapping > NIS Group Accounts**.
2. Click on **NIS Service**.
3. Check or clear **Enable NIS**. If you are enabling NIS, enter the:
   - master server’s IP address in the **NIS Server** field.
   - appropriate NIS domain name in the **NIS Domain** field.
4. Click **Apply**. You do not need to restart the system.

The NIS files are automatically updated every 5 minutes when the NIS service is enabled. If the service is disabled, you see either stale data or an informational message indicating that the file is empty.

Note	The NIS service can be enabled from either the NIS User Account page or the NIS Group Account page.

NIS Service

Note	The HP NetStorage 6000 supports NIS service, but not NIS+ service.

The HP NetStorage 6000 allows you read-only, online access to the user NIS file generated by the Network Information Services (NIS) service. In order to see this file the NIS service must first be enabled.

To enable or disable NIS (disabled is the default) for User Accounts:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **User Mapping > NIS User Accounts** *or* **User Mapping > NIS Group Accounts**.
2. Click on **NIS Service**.
3. Check or clear **Enable NIS**. If you are enabling NIS, enter the:
   - master server's IP address in the **NIS Server** field.
   - appropriate NIS domain name in the **NIS Domain** field.
4. Click **Apply**. You do not need to restart the system.

The NIS files are automatically updated every 5 minutes when the NIS service is enabled. If the service is disabled you see either stale data or an informational message indicating that the file is empty.

Modifying the User Map File

The user map file contains an entry for each unique Windows client that attaches to the HP NetStorage 6000 while the device is configured to use user-level security. The format of the file entry is:

```
<UNIX username>:<UID>:<NT username>:<NT domain>:<NT RID>
```

The UID value that is assigned to the Windows client is one number larger than the largest UID value in the users map or users NIS file starting with number 65537. The default UNIX username is the UID value prefixed with a lower case **u**.

When a new Windows client attaches to the HP NetStorage 6000 this file is consulted along with the mapping strategy that you have selected. For example, if you have selected User Name mapping, when a UNIX client attaches with the an identical UNIX and Windows username the UNIX client information is used instead of the default information discussed above.

By reviewing the user map file you see that the UNIX usernames, UIDs and Window client information is associated with the file security for each protocol.

To add or modify an entry in the user map file:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **User Mapping** > **User Map File**. The current user map file is displayed.
2. Click **Modify Map**. The UNIX Logon Name and UNIX UID values are displayed and can be edited. The Windows Logon Name, Windows Domain, and Windows RID values are displayed for informational purposes only and cannot be edited.
3. Once you have completed your modifications, click **Apply** to return to the User Map File page. You do not need to restart the system.

To delete an existing map file entry:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **User Mapping** > **User Map File**. The current user map file is displayed.
2. Click **Delete Map**. You receive confirmation that the selected user has been deleted.

Modifying the Group Map File

The group map file contains an entry for each unique Windows primary group that is associated with the Windows users that access the NetStorage 6000 when it is configured to use user-level security. The format for the group map file is:

```
<UNIX groupname>:<GID>:<NT groupname>:<NT
domain>:<NT RID>
```

The GID value that is assigned to the Windows clients' primary group is one number larger than the largest group map or group NIS file starting with number 65537. The default UNIX groupname is the GID value prefixed with a lower case **u**.

When a Windows client attaches to the NetStorage 6000 for the first time this group map file is consulted along with the group mapping strategy that has been selected. For example, if you have selected group mapping by name, when a UNIX client attaches with an identical UNIX and Windows group name, the UNIX group information is used instead of the default group information discussed above.

To modify an entry in the group map file:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **User Mapping** > **Group Map File**. The current group map file is displayed.
2. Click **Modify Map**. The UNIX group name and UNIX GID values are displayed and can be edited. The Windows Group Name, Windows Domain, and Windows RID values are displayed for informational purposes only and cannot be changed.
3. Once you have completed your modifications, click **Apply** to return to the User Map File page. You do not need to restart the system.

To delete an existing map file entry:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **User Mapping** > **Group Map File**. The current group map file is displayed.
2. Click **Delete Map**. You receive confirmation that the selected group has been deleted.

Shutting Down and Restarting

Shutting Down the HP NetStorage 6000

Shut down the device if you:

- move the device to a new location
- anticipate a power outage in your building and you do not have an uninterruptible power supply for the device

To shut down the device:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Shutdown/Restart**.
2. Click the **Shutdown** button. A dialog box informs you that:
   - You and any other connected users will lose the connection to the device.
   - The NetStorage web interface in the current browser cache becomes invalid. The browser closes and you must re-connect to the system after it reboots.
3. Click **OK**.
4. When the LCD display on the unit is blank, turn off the device by pushing the power switch in the back.

Restarting the HP NetStorage 6000

Restart the device if you:

- Download a new version of the NetStorage web interface as described in “Upgrading From the Web” on page 9-4.
- Install a new operating system
- Change your security mode as described in “Windows Settings” on page 3-6.
- Enable DHCP as described in “TCP/IP Settings” on page 3-2.

To restart the device:

1. Using the NetStorage web interface, click the **Configuration** tab, then select **Shutdown/Restart**.
2. Click the **Restart** button. A dialog box informs you that:
   - You and any other connected users will lose the connection to the device.
   - The NetStorage web interface in the current browser cache becomes invalid. The browser closes and you must re-connect to the system after it reboots.
3. Click **OK**.

Chapter 4
Managing Storage

The Storage Tab

The storage tab in the HP NetStorage 6000 lets you:

- View file volumes and share information
- Manage file volumes (create, expand, rename, and delete)
- Manage directories in file volumes (create, rename, and delete)
- Manage Windows shares in directories (create or edit)
- Manage mount points (UNIX only)
- View physical drive information
- View logical drive information
- Manage logical drives (create, delete, and rebuild)
- Assign hot spare drives

Managing Physical and Logical Drives

View Physical Drive Information

The HP NetStorage 6000 contains ten drive bays to host as many as ten physical disk drives. Physical drives are used in groups of three to eight to create RAID sets (logical drives). Physical drives are also used individually as hot spares. A drive assigned as a hot spare automatically repairs a RAID set when one of the drives in the set becomes damaged or is removed.

To examine and manage physical drives:

Using the NetStorage web interface, click the **Storage** tab, then select **Physical Drives**.

A table displays the following drive information.

- Slot assignment of each drive
- Vendor or manufacturer of the drives
- Product drive name
- Revision level of the drive
- Serial number of the drive
- Drive capacity in Megabytes
- Mapping of the Logical Drive associated with the physical drive

The table also shows the current status of each drive:

- Empty
- Rebuilding
- Online
- Unassigned
- Hot Spare
- Dead

Note	The **Actions** button in the upper left corner lets you create logical drives and assign hot spares.

View Logical Drive Information

Logical drives on the HP NetStorage 6000 are roughly equivalent to what is commonly referred to as a RAID set. You may partition the storage space on logical drives to create up to four file volumes. You may want to view logical drive information to see how much free space is available in the individual partitions, and where you might want to save your data.

To manage and view logical drive information:

Using the NetStorage web interface, click the **Storage** tab, then select **Logical Drives**.

A table displays partition information for each logical drive in the system. To the left of the table, the following drive information displays:

- Drive name
- Drive capacity
- RAID level
- Drive status

The table contains partition information for the logical drive. Each logical drive contains a maximum of four partitions. Partitions are allocated to create file volumes. The table displays the current allocation of partitions to the file volumes on the system, and contains the following information:

- Partition number (1 through 4)
- File volume name
- Raw capacity (unformatted capacity dedicated to the file volume)
- Percent of total space used by the partition

Partitions that are available for the creation of new file volumes display <FREE SPACE> in the **File Volume Name** column, and show the maximum available free space in the **Raw Capacity** column.

Note	The **Actions** button in the upper left corner lets you create, rename, expand, and delete file volumes.

Create a Logical Drive

You create logical drives by grouping a set of physical drives into a single RAID set. Currently, the HP NetStorage 6000 supports only RAID level 5 for the creation of logical drives. Because RAID level 5 requires a minimum of three physical drives for a RAID set, the HP NetStorage 6000 requires at least three drives to be grouped together to create a logical drive.

To create a new logical drive:

1. Using the NetStorage web interface, click the **Storage** tab, then select **Physical Drives**.
2. Click **Actions**, then select **Create Logical Drive**. All of the physical drives in the system are displayed. Each drive is represented by a graphic of a drive bay:
   - Drive bays containing unassigned drives are selectable.
   - Drive bays that are empty, or that contain assigned drives are not selectable.
3. Click on the graphics of the drives that are to be used to make the new logical drive.
4. Click **OK**.

A status message is displayed along with a progress bar and a **Close** button. You do not need to monitor the creation process, and you may return to the **Physical Drives** screen at any time by pressing the **Close** button. To return to the progress screen, select **Actions > View Create Status**.

The drive is prepared in three stages:

1. The command is issued to the RAID controller.
2. The RAID controller activates the new logical drive.
3. The logical drive is initialized.

The first two steps execute quickly and are typically completed within a minute. After these two steps are complete, the new Logical Drive is ready to use. At this point, you may create volumes and place data on those volumes. You do not need to wait for the third step to run to completion.

Drive Initialization, the third and final step of Logical Drive creation, takes place in the background and may be time-consuming. This process should run to completion before the system is re-booted or powered down. In order for the system to track the process, other RAID-related operations, such as Hot Spare assignment, are not allowed until this process is complete.

Note	A logical drive may contain a maximum of eight physical drives.

Delete a Logical Drive

When you delete a logical drive, the physical drives it used are set to the unassigned state. It is important to note though, that you can only delete the *last* logical drive in the list. For example, if two logical drives exist on the system, in order to delete the first logical drive, you must first delete the second logical drive.

To delete a logical drive:

1. Using the NetStorage web interface, click the **Storage** tab, then select **Physical Drives**.
2. Click **Actions**, then select **Delete Logical Drive**.
3. The logical drive available for deletion displays.
4. If it is the drive you want to delete, click **Yes**. Otherwise, click **No**.
5. If you click **Yes**, a second page appears to confirm your selection. **Caution:** Verify that this is the drive you want to delete. Deleting a logical drive destroys all the data on that logical drive, and the procedure cannot be reversed.
6. Enter `Yes`.
7. Click **OK**.

Note	While the HP NetStorage 6000 deletes a drive, the LEDs flash and the user interface freezes. Do not perform any tasks with the keyboard or mouse while this activity takes place.

Rebuild a Logical Drive (RAID set)

If a physical drive in a logical drive fails and a hot spare is not available to automatically replace it, the logical drive goes into a critical state. In this state, the logical drive does not protect the data with redundancy. All data on the logical drive is lost if another drive fails.

Note If you replace a failed drive with a new drive, you must use the same slot that the failed drive used.

To recover the logical drive from critical state, replace the failed hard drive with a new one and rebuild the logical drive:

1. Replace the failed drive. (Follow the instructions that come with the drive.)
2. Using the NetStorage web interface, click the **Storage** tab, then select **Physical Drives**.
3. Verify that the drive is recognized by the system. Click **Actions**, then select **Refresh** to update the table. If the drive is not recognized (as unassigned), reboot the system.
4. Once the drive is recognized and is in an unassigned state, click **Actions**, then select **Rebuild Logical Drive**.
5. You are prompted to select a logical drive to rebuild. Normally, there is only one drive to select. Select the desired logical drive to rebuild.
6. Click **OK**.

The rebuilding process may take one or more hours. To monitor the status of the drive on the **Physical Drives** page, click **Actions**, then select **Refresh** to update the table. When the drive is rebuilt, its status changes from *Rebuilding* to *Online*.

Assign a Hot Spare

The HP NetStorage 6000 lets you assign physical drives to function as hot spares. Hot spare drives are reserved drives that are used only when a physical drive that is part of a logical drive fails. When this happens, the system automatically selects the first available hot spare drive to take the place of the failed drive. The logical drive is rebuilt using the hot spare, and the hot spare drive becomes a member of the logical drive.

Once a hot spare is used to repair a logical drive, its assignment changes from *Hot Spare* to *Online*. If you replace the failed drive, it automatically receives an assignment of *Unassigned*. You must manually assign the new drive to *Hot Spare* if the new drive is to serve as a hot spare.

Most systems only use one physical drive to serve as a hot spare. However, there is no restriction on the number of hot spares in the system, though every additional hot spare uses another physical drive and lessens storage capacity. Any and all drives may serve as hot spares. There is no requirement to have a hot spare on the system at all.

To assign a hot spare:

1. Click the **Storage** tab, then select **Physical Drives**.
2. Click **Actions**, then select **Assign Hot Spares**.
3. A picture representing all of the physical drives in the system appears. Each drive is represented by a graphic of a drive bay. Drive bays containing unassigned drives or hot spare drives are selectable. All other drive bays are not selectable.
4. Select the drives to be used as hot spares by clicking on them.
5. Click **OK**.

Note	Refer to the HP support web page for more information on upgrading storage capacity or replacing a failed hard drive.

Managing File Volumes and Directories

View File Volume Information

File Volumes are the basic unit of logical storage for a file system on the HP NetStorage 6000. The volume contains a directory hierarchy that stores files within the directories of that hierarchy. You can manage directories and files from a remote UNIX or Windows system using Explorer on Microsoft Windows, or by mounting the file volume from a UNIX shell. The HP NetStorage 6000 also offers a simple browsing tool that allows you to examine the hierarchy of each file volume on the system, and to perform basic management functions.

To view file volume information:

1. Using the NetStorage web interface, click the **Storage** tab, then select **File Volumes**. A tree list appears on the left. On the right, a file volume summary screen appears. This summary screen displays the following general information for each volume on the system:
   - File volume name
   - Total capacity in MB
   - Free space in MB
   - Free space in percent
   - Used space
2. Navigate the tree list to display more detailed information for each file volume, and each subdirectory within the file volume. The root of the tree is an image of a computer, and is called **Summary**. Select this to display the summary page.
   File volumes are displayed in the second level of the tree hierarchy. Select a file volume to display a page that contains the following information:
   - File volume name
   - Total capacity in MB
   - Used space in MB
   - Used space in percent
   - Unused space in MB
   - Unused space in percent
   - Windows share status of the volume root, and lets you change the share status. You can use the **Actions** button to manage directories.

3 To view subdirectory information, select a subdirectory (designated by a file folder graphic). The following information displays:

- Name of subdirectory
- Absolute path from the root
- Windows share status

Create a New File Volume

You create file volumes by allocating space from a logical drive. Logical drives on the HP NetStorage 6000 are divided into a maximum of four partitions. Whenever you create a file volume, it uses one partition on one logical drive.

To create a new file volume:

1 Using the NetStorage web interface, click the **Storage** tab, then select **Logical Drives**.

2 Click **Actions**, then select **Create File Volume**.

3 Enter a new file volume name in the space provided.

4 Select a partition to use from the pull down menu.

5 Enter desired file volume size (MB) in the space provided.

6 Click **OK**.

A progress bar displays while the new volume is formatted.

Expand a File Volume

To expand a file volume, there must be free storage space and a free partition on a logical drive. This free space and free partition do *not* need to be on the same logical drive as the file volume to be expanded—you can create file volumes that span across logical drives. This gives you the option of expanding existing volumes by installing another logical drive on the system.

To expand an existing file volume:

1. Using the NetStorage web interface, click the **Storage** tab, then select **Logical Drives**.
2. Click **Actions**, then select **Expand File Volume**.
3. Select the volume to be expanded.
4. Select a partition to use from the pull down menu.
5. Enter desired file volume size in the space provided.
6. Click **OK**.

A progress bar displays while the file volume is expanded.

Rename a File Volume

To rename a file volume:

1. Using the NetStorage web interface, click the **Storage** tab, then select **Logical Drives**.
2. Click **Actions**, then select **Rename File Volume**.
3. Select the volume you want to rename.
4. Enter a new name in the text field.
5. Click **OK**.

Note	You can not rename file volumes that have been expanded.

Delete a File Volume

When you delete a file volume, the space it used is reclaimed by the logical drive. However, if you delete a file volume that uses a partition number lower than a partition currently in use by another file volume, the freed space is not combined with the other free space on the logical drive.

For example, if partition 1 is deleted, and partition 2 contains a file volume, then the space freed up by partition 1 must remain as the fixed space of that partition. Partition 1 can still be used for a file volume, but the volume must allocate no more space than the volume that was deleted.

This restriction does not apply to deleted file volumes that are located in partitions adjacent to the remaining free space on the logical drive.

Caution Deleting a file volume destroys all the data on that volume. The procedure cannot be reversed.

To delete a file volume:

1. Using the NetStorage web interface, click the **Storage** tab, then select **Logical Drives**.
2. Click **Actions**, then select **Delete File Volume**.
3. Select the volume you want to delete.
4. Click **OK**.
5. Enter `Yes` when asked to confirm your selection.
6. Click **OK**.

Create a Directory

You can create subdirectories under the root level of the file volume, or under any directory in the hierarchy. Subdirectories let you organize your data into easily accessible folders.

To create a directory:

1. Using the NetStorage web interface, click the **Storage** tab, then select **File Volumes**.
2. Navigate the tree list to highlight the desired file volume or directory.
3. Click **Actions**, then select **Create Directory**.
4. Enter the directory name in the text field.
5. Click **OK**. The new directory is created immediately.

Note Before a network user can see this directory, you must either share it or create a mount point. For more information, see “Create or Edit Windows Shares” on page 4-14.

Rename a Directory

To rename a directory:

1. Using the NetStorage web interface, click the **Storage** tab, then select **File Volumes**.
2. Navigate the tree list to highlight the desired directory.
3. Click **Actions**, then select **Rename**.
4. Enter a new name in the text field.
5. Click **OK**.

Delete a Directory

You can delete directories to free up disk space or to remove unwanted data on the HP NetStorage 6000.

Caution	Deleting a directory destroys all the data in that directory and all of its subdirectories. The procedure cannot be reversed.

To delete a directory:

1. Using the NetStorage web interface, click the **Storage** tab, then select **File Volumes**.
2. Navigate the tree list to the desired directory item and select it.
3. Click **Actions**, then select **Delete**.
4. When prompted, confirm your selection.

Allowing Access to Data

Create or Edit Windows Shares

Shares are permissions that let you control Microsoft Windows users' access to data. You can create shares in any directory within a file volume, including the root. Once a share is created, users may attach to the share via the network neighborhood in Windows and store and retrieve files and directories.

Security for network shares is handled in one of two ways:

- **Secure share level security** is the simplest security method available. Access to the share may be restricted on a share by share basis. The administrator can set Read Only passwords and Read/Write passwords for each share on the system. Users wishing to gain access to a share are asked to supply the correct password. Only users with the correct password are given access to the share. Passwords are encrypted for transmission over the network lines.
- **User level security** is more advanced and offers more flexibility for both the administrator and the user:
  - Users are authenticated via the NT domain controller using pass through authentication.
  - Users accessing the resources of the system must be logged onto an NT domain and must have specific rights to access the given resource. The resource is not only the share, but the directories and files within the share as well.
  - Administrators and users may restrict access to any file, directory or groups of files and directories to any user or group of users in the domain.

To create or edit shares in Windows:

1. Using the NetStorage web interface, click the **Storage** tab, then select **File Volumes**.
2. Select the item to be shared in the tree list (the file volume root or a subdirectory).
3. In the **Windows Networking** box, select **Share As**.
4. A default name appears in the **Share Name** field. You can change this name to any name desired.

5 Enter a **Comment** (optional).

6 Enter a password in the R/O and R/W fields. (These appear only if you are using Share Level Security. See “Share-Level Security” on page 8-5.)

7 Click **Apply**.

Note	Windows shares are indicated in the tree list with a graphic of a hand holding the shared object.

Edit Host Access

The HP NetStorage 6000 automatically generates a UNIX mount point at the root of the file volume when you create the volume. Mount points allow access to the system via the NFS protocol. By default, the mount point allows no access from any UNIX host when the volume is created. You must specifically grant access before UNIX host systems can mount the volume. Host access rights to resources via the NFS protocol are managed through the approve file.

The /etc/approve File

In traditional UNIX implementations, the `exports` file is used to restrict host access to the defined mount points. On the HP NetStorage 6000, this function is handled by the `/etc/approve` file. The administrator may edit this file:

- Directly from a text editor via an NFS (UNIX) mount or a Windows share. The file is named `approve`, and is located in the `/etc` directory in the first file volume created on the system. The `/etc` directory is an administrative file directory. The files may be edited (with the correct permissions), but they cannot be deleted.
- From the HP NetStorage web interface, as explained in this section.

Entries in the approve file have four fields:

Field	Restrictions
class	This field specifies the class of object to protect. In all cases, the object is **files**.
specifier	This field specifies the resources on the NetStorage 6000 server to protect. For example, /engineering, applies to all files and directories in the `/engineering` file system.
host pattern	This field has the name of a host or group of hosts that have access rights. Host names must be resolvable through the local `/etc/hosts` file, the NIS hosts file, or through DNS. Groups of hosts are specified in the `/etc/hostgrps` file. If the host pattern is the name of a group, then it must be preceded by the @ symbol. The wildcard character (*) may be used to specify all hosts. Note that the `@general` group is a pre-defined group that specifies all hosts.
rights	This field specifies the access limits to apply. The entry in this field can be: **access=rw** Allow read and write access to the resources **access=ro** Allow read only access to the resources **access=none** Deny all access to the resource

The fields must be separated by one or more spaces or tabs. If a specifier contains space characters (such as a directory name that contains spaces), then the entire specifier must be enclosed in double quotes.

Whenever a host attempts to mount a volume, the approve file is searched to determine the appropriate access to grant the host. The file is searched sequentially from top to bottom. When a match is found to the host pattern and the volume specifier, then the associated access rights are applied. All entries in the file after the matched entry are ignored. Therefore, it is important to order the entries in the file so that the more specific entries are listed first, and the more general entries are listed last.

Here is a list of sample entries in the host access file:

```
#class  specifier       host pattern  rights
files   /acct/usr       it0           access=rw
files   /acct/usr       @guest        access=ro
files   /acct/etc       it1           access=rw
files   /acct/etc       it2           access=rw
files   /acct           @general      access=none
```

These five entries define the access to the `/acct` volume. In particular, the first two entries define access to the `/acct/usr` directory. Read only access is granted to the `guest` group (defined in the `/etc/hostgrps` file). The next two entries allow read/write access to the machines `it1` and `it2` to all files and directories in the `/acct/etc` directory. The last entry is a catch-all, indicating that all other hosts have no access to the `/acct` volume.

The following list demonstrates the use of wildcards and DNS domains:

```
#class  specifier host pattern       rights
files   /engineering *.eng.nas.hp.com access=rw
files   /engineering *.test.nas.hp.com access=ro
files   /engineering @general        access=none
files   /        @general            access=none
```

The first three entries define the access allowed to the `/engineering` volume. The wildcard (*) character was used to specify all the machines in a DNS domain. The last two lines in the examples are catch-alls, indicating that all other hosts have no access to the `/engineering` volume or any other volume. These entries are optional since access is always denied if it is not specifically granted.

To view and edit the host access file using the NetStorage web interface:

1. Using the NetStorage web interface, click the **Storage** tab, then select **Host Access**.
2. Modify the file as you would in any text editor.
3. Click **Save Changes** when you are done editing.

Note If there is no entry in the approve file to define access to a volume, then access is denied to all hosts. The root user, mounting from a Trusted Host, always has full read/write access to all volumes, regardless of the access rights specified in the approve file.

The /etc/hostgrps File

In most cases, you want to specify a group of computers when identifying Host Access to the NetStorage 6000. In many of these situations, the wildcard character (*) serves this purpose. However, in some cases it is not sufficient. You can get around this problem by simply generating a Host Access entry for each computer, or you can define a group of host computers that may then be referenced by name (preceded by the @ symbol). A group of host computers may be defined by creating an entry in the `/etc/hostgrps` file. The file must be edited manually, using a text editor via the NFS protocol, or the CIFS protocol (assuming that you have the proper rights).

Groups may be created by adding an entry into the `/etc/hostgrps` file. Each entry starts with the name of the group, followed by a sequence of host names to associate with the group. Every name is delimited by a space character. For example:

```
# Hostgrps file (group hosts under a name for access control)
general *
mygroup eng6284.stor.hp.com eng6a2c.stor.hp.com
eng8106.stor.hp.co
mygroup 10.58.159.245 hpcust6da6
```

Note The host names may appear as fully qualified domain names, IP addresses, or host names as they appear in DNS or a hosts file. Entries for a group may span more than one line by entering the group name again at the beginning of the next line.

The host names must be resolvable through the hosts file, the NIS hosts file, or DNS.

Chapter 5
Backing Up and Restoring Files

The Backup and Restore Tab

The Backup and Restore tab lets you:

- Create disk checkpoints
- Modify checkpoint schedules
- Manage disk checkpoints
- View the tape backup job status
- View the tape restore job status
- View the tape magazine
- View the tape log
- Create and execute backup jobs
- Choose your backup options
- Back up checkpoints
- Restore volumes
- Restore files and directories
- Check your tape settings

Note	Labeling your tapes and keeping track of schedules is a crucial component in the backup and restore process.

Using the HP SureStore 818 or 1/9 DLT Autoloader

HP designs the HP NetStorage 6000 to work with the HP SureStore 818 (part number C6284NB) or Autoloader 1/9 (part number C7146NB) DLT backup devices. See the installation poster for directions on attaching the Autoloader to the HP NetStorage 6000.

Contact your local HP Authorized Reseller for information about ordering either the 818 or 1/9 HP SureStore DLT Autoloader. If you already own either Autoloader, purchase a SCSI cable (part number D6020A) to connect your Autoloader to the HP NetStorage 6000. If you do not have a reseller, log on to the HP web site www.hp.com or call 1-800-826-4111 to locate the one nearest you.

You should refer to your User's Guide that came with your Autoloader for information about setup and maintenance. The information in this chapter is for the Autoloader 818. If you have the 1/9 Autoloader and you are unable to find your user documentation, refer to the HP web site.

The 818 Autoloader has eight slots: Slots 1-6 are in the front of the unit and Slots 7 and 8 are inside.

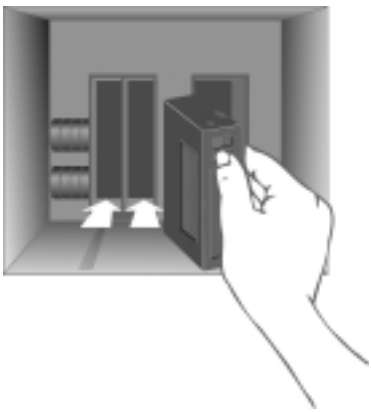
Note The Autoloader cannot detect the difference between a cleaning tape and a tape cartridge, so use caution when loading tapes into the magazine.

Loading Tapes into the Magazine

With the tape's write-protect switch facing out and the smooth edge facing the top of the magazine, insert the tape until it clicks. A metal tab releases to lock the tape into place.	
When you load tapes to perform a backup, the Autoloader does not care about previous tape contents; it treats every tape in the magazine as blank. Be sure to sequentially label your tapes after a backup. If you are restoring a specific file or your entire system, you must load the tapes in the correct order into the magazine.	

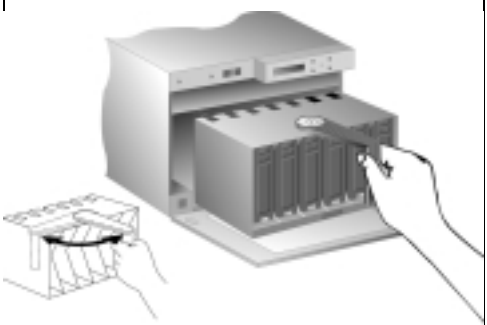
Loading Tapes into the Internal Slots

To load internal tapes, remove the magazine from the Autoloader. With the tape's write-protect switch facing out of the Autoloader and the smooth edge facing the top of the slot, insert the tape until it clicks into place.



Loading the Magazine into the Autoloader

With the handle facing out of the Autoloader, insert the magazine into the Autoloader. Slide the magazine in until it clicks into place. Slide the handle all the way to the left to store the magazine.



Cleaning the Autoloader Tape Drive

The drive mechanism should only be cleaned if `CLEAN DRIVE` displays on the front panel. For directions on how to clean your tape drive, see the *HP SureStore DLT Autoloader User's Guide*.

Ordering Tapes

You can order a full range of supplies through a Hewlett-Packard authorized dealer, an HP sales office, or HP Direct. To contact HP Direct, call 1-800-227-8164. See the list below for product names and part numbers.

- Data cartridge (C5141-85701)
- Cleaning cartridge (C5142-85700)

Local and Remote Backups

Backup Overview

Although the HP NetStorage 6000 provides RAID 5 hardware protection for your data, a backup strategy can prevent data loss in cases of inadvertent deletion or system disasters such as theft and fire. Using features built-in to your HP NetStorage 6000, a backup strategy can provide:

- Daily checkpoints for rapid recovery of individual files or directories, plus. See "Creating Checkpoints" on page 5-9.
- Full backups on a weekly schedule for long-term storage and disaster recovery. See "Creating and Executing Backup Jobs" on page 5-14.

To perform backups, you need to attach either an 818 or 1/9 HP SureStore DLT Autoloader to your HP NetStorage 6000 (see the installation poster for instructions). You can set up the tape device to perform two types of backups:

- A local backup: Use the backup application in the NetStorage web interface plus an optional 818 or 1/9 HP SureStore DLT Autoloader. See "Performing a Local Backup" on page 5-5.
- A remote backup: Use one of several popular network remote backup applications on a networked computer. See "Performing a Remote Backup" on page 5-6.

Note	You do not need to format tapes for a backup. However, before you load tapes in the Autoloader, make sure they are not write-protected.

The length of time required to perform a backup depends on the size of the volume and the local area network (LAN). As a general rule:

- For a local backup, the Autoloader backs up 25 gigabytes per hour.
- For a remote backup on a 10Base-T network, the Autoloader backs up 3 gigabytes per hour.
- For a remote backup on a 100Base-T network, the Autoloader backs up 10 gigabytes per hour.

During a backup, the Autoloader's control panel displays `Writing` and the green activity light flashes.

Performing a Local Backup

Use the backup application in the NetStorage web interface plus an optional 818 or 1/9 HP SureStore DLT Autoloader to perform a local backup. See the installation poster for directions on attaching the Autoloader to the HP NetStorage 6000 and see "Using the HP SureStore 818 or 1/9 DLT Autoloader" on page 5-1 for information on using the Autoloader.

Note	You can only access **Tape Status**, **Tape Backup**, **Tape Restore**, and **Tape Settings** in the **Backup/Restore** tab *after* you attach an Autoloader to your HP NetStorage 6000

In a local backup session, a special checkpoint of your data is first created on disk, then the data is transferred to the locally attached Autoloader. The checkpoint uses only a small amount of disk space and the data transfer does not interfere with your LAN traffic.

To run a local backup:

1. From your workstation, open a web browser and enter the IP address of the HP NetStorage 6000.
2. Click the **Backup/Restore** tab, then select **Tape Backup** (see "Creating and Executing Backup Jobs" on page 5-14 for more information).

The local backup feature provides simple scheduling capability and can be configured to back up individual files or combinations of volumes.

Performing a Local Restore

From a local backup tape, a restore operation can select an individual volume, directory, or file. Make sure you carefully label and date your local backup tapes because a database of local backup operations is not maintained.

To run a local restore:

1. From your workstation, open a web browser and enter the IP address of the HP NetStorage 6000.
2. Select the **Backup/Restore** tab, then click **Tape Restore** (see "Restoring Volumes" on page 5-18 or "Restoring Files and Directories" on page 5-20 for more information).

Performing a Remote Backup

Use third-party backup applications on any computer on the network with a tape drive attached to perform a remote backup.

When you run a remote backup, data from the HP NetStorage 6000 transfers over the network to the remote server running the backup application, and then to the server-attached tape device. The remote backup application cannot control the Autoloader connected to the HP NetStorage 6000.

If the backup application is running under NT, the restore operation recovers both the NT and UNIX security settings for each file. If the backup application is running under UNIX, the restored NT files revert to the default user security setting, while UNIX files retain their full security settings.

See "Remote Backup Applications Overview" on page 11-1 for a list of remote backup applications the HP NetStorage 6000 integrates with.

Disk Checkpoints

What Are Disk Checkpoints?

You can use the disk checkpoint feature to create a read-only *virtual* copy of your volume. This copy does not consume the equivalent disk space that an actual copy consumes. Because they are not real copies, checkpoints appear as a collection of directories in a *virtual volume*. This volume has the same name as the original volume but with a `.chkpnt` extension. You can retrieve data from the checkpoint by browsing to the data you need and copying it to the desired location. You can also back up checkpoints to tape. For more information, see "Backing Up Checkpoints" on page 5-17.

You can create checkpoints manually (by checking **Immediate**) or have them created automatically at scheduled times by checking the appropriate boxes. The following table lists the checkpoints you can schedule and their deletion dates.

Checkpoint	Creation Time	Deletion
Immediate	Now	Delete manually
Weekly	Every Sunday at 1 am	Automatically deletes in 14 days
Nightly	Every weekday at 1 am	Automatically deletes in 7 days
Daily	Every weekday at 1 pm	Automatically deletes in 3 days
Every three hours	Every weekday from 9 am to 6 pm	Automatically deletes in 6 hours

You name immediate checkpoints. The system names scheduled checkpoints based on the creation date and time and their deletion date.

For example, if you created a three-hour scheduled checkpoint on January 19, 2000 at 9 am, the system names that checkpoint `20000119-090001,6h`. The date of this checkpoint is year 2000, month 01, day 19, and the time you created it was 09 am, 00 min, 01 seconds. The checkpoint deletes in 6 hours.

If you do not want the system to delete the checkpoint on its deletion time, rename the checkpoint (see "Renaming or Deleting Checkpoints" on page 5-10). The name of the checkpoint is also the name of its directory on the virtual volume.

Note When checkpoints are created, they do not use much disk space. As you make changes to the disk volume, checkpoints use increasing amounts of space. Checkpoints may be deleted automatically if the system begins to run out of disk space. To save disk space, delete old checkpoints periodically.

Checkpoints appear as a directory in the virtual volume. For example, if you have two checkpoints for volume X (one you created named ABC and a scheduled checkpoint named 20000119-090001,6h), you would find the following on the virtual volume:

```
/X.chkpnt/ABC (your checkpoint)
/X.chkpnt/20000119-090001,6h (scheduled checkpoint)
```

Checkpoints have benefits and limitations.

Benefits	Limitations
• Fast, accurate, and convenient file archive. • Quick and easy archive retrieval. • Uses minimal disk space initially.	• Depends on the disk not failing. • Uses increasing amounts of storage over time.

Creating Checkpoints

To create a new checkpoint:

1. Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Disk Checkpoints > Create/Schedule New Checkpoints**.
2. Select a volume from the drop-down list.

To create a checkpoint now:

1. Click the box next to **Immediate.**
2. Type a name for the checkpoint.
3. Click **Save Settings** and respond to the confirmation dialog box. The checkpoint is saved to the volume.

To schedule automatic creation of checkpoints:

1. Click the box or boxes next to all desired schedules.
2. Click **Save Settings**, then click **OK** to save your changes.

Note	You name the immediate checkpoints. The system names the scheduled checkpoints based on the creation date and time and their deletion date.

Modifying Checkpoint Schedules

To modify the checkpoint schedule:

1. Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Disk Checkpoints > Create/Schedule New Checkpoints**.
2. From the drop-down list, select the volume whose schedule you want to modify.
3. Click the box or boxes to change the schedule of the checkpoint(s).

Note	You can select any schedule you desire (for example, one, several, or all the scheduled settings).

4. Click **Save Settings**. A dialog box asks you if you want to save your changes. Click **OK**.

Managing Checkpoints

Note	To save disk space, delete old checkpoints periodically.

To access the data in a checkpoint:

1. Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Disk Checkpoints > Manage Existing Checkpoints**.
2. Select a volume from the drop-down list.
3. Choose a checkpoint to retrieve the checkpoint name and directory.
4. Locate the directory where the checkpoint resides and give yourself permission to access the directory.

Renaming or Deleting Checkpoints

Checkpoints that are created at a scheduled time are automatically deleted based on their creation date. The system parses the filename to determine when to delete the checkpoint. If you do not want the system to delete the checkpoint on its deletion date, rename the checkpoint.

To rename or delete a checkpoint:

Note	Renamed checkpoints may still be deleted if the file system starts to run out of disk space.

1. Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Disk Checkpoints > Manage Existing Checkpoints**.
2. Select a volume from the drop-down list.
3. Choose the checkpoint you want to rename or delete.
4. Check either:
   - **Rename checkpoint**, enter a new name, then click **Apply**.
   - **Delete Checkpoint,** and respond to the confirmation dialog box.

Checking the Current Tape Drive Status

Tape Backup Job Status

The **Tape Backup Job Status** screen displays the status of your current or last backup job.

To view this screen using the NetStorage web interface:

1. Click the **Backup/Restore** tab.
2. Select **Tape Status > Backup Job Status**.

The fields are:

Field	Description
Device Status	`Ready`, `Backup Running`, `Restore Running`, `Testing a Tape`, or `Unknown`.
Job Name	Name you have given the backup job.
Job Status	In progress or complete.
Errors	Number of errors that occurred during the job. To view the error log for this tape, click **Tape Log**.
Job Start Time	Date and time the job began.
Job End Time	Date and time the job finished.
Job Length in Minutes	Time it took to complete the job.
Files Processed	Number of files processed.
Bytes Processed	Number of bytes processed.
Tapes Used	Number of tapes the job required.

Note Make sure you view the tape log when the job completes to determine which tapes were written to. This procedure is the only way to know which tapes were used. Remove those tapes from the Autoloader and label them. For more information, see “Tape Log” on page 5-14.

The screen refreshes every 10 seconds.

Tape Restore Job Status

The **Tape Restore Job Status** screen displays the status of your current or last restore job.

To view this screen using the NetStorage web interface:

1. Click the **Backup/Restore** tab.
2. Select **Tape Status** > **Restore Job Status**.

The fields are:

Field	Description
Device Status	`Ready`, `Backup Running`, `Restore Running`, `Testing a Tape`, or `Unknown`.
Job Status	In progress or complete.
Errors	Number of errors that occurred during the job. To view the error log for this tape, click **Tape Log**.
Job Start Time	Date and time the job began.
Job End Time	Date and time the job finished.
Job Length in Minutes	Time it took to complete the job.
Files Processed	Number of files processed.
Bytes Processed	Number of bytes processed.
Tapes Used	Number of tapes the job required.

The screen refreshes every 10 seconds.

Tape Magazine

The **View Tape Magazine** screen displays information about the tape device attached to your HP NetStorage 6000. You can not retrieve information on a tape if:

- the device is busy
- you do not have a tape device attached
- an error has occurred on your system

Before performing a backup or a restore, make sure you:

- **(Restore only)** Write-protect all restore tapes before loading them into the magazine. Slide the write-protect switch until it clicks and an orange tab appears.
- Verify information about the tapes you loaded in the slots by clicking on the tape icon below the tape's slot number.
- Test the slot containing the first tape of the set from which you want to restore.

Note	Loading and reading a tape takes at least three minutes.

To obtain information about a tape:

1. Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Tape Status** > **Tape Magazine**.
2. To read the tape information, click on a tape icon below the tape's slot number. If a backup, restore or other activity is taking place, the tape icons are inaccessible.
3. A dialog box informs you that the device is testing the slot you selected. Click **OK**.
4. The following information about the tape appears on the screen if the tape contains a backup:
   - slot number being tested
   - job on the tape
   - serial number of the tape
   - order of the tape within the job
   - type of backup performed (if you are testing the first tape of a job)
   - date and time you created the tape
   - volumes on the tape (if you are testing the first tape of a job)
5. Review the information on the screen. If you want, you can test another slot.

Tape Log

The tape log tells you which tapes were written to during a backup, as well as the date, time, and description of events that occurred.

To display the tape log for your tape drive:

1. Using the NetStorage web interface, click on the **Backup/Restore** tab, then select **Tape Status** > **Tape Log**.
2. A screen displays the events on the backup tape. If a backup is in progress, click **Bottom** to see the most recent information in the tape log.

You can get more information from the tape log by clicking on the buttons labeled **Top**, **PgUp**, **PgDn**, and **Bottom**.

Backing Up

Creating and Executing Backup Jobs

You can only back up *volumes* to your backup device, not *individual files* or *directories*. You can store only one backup job on a tape, regardless of how much data you are backing up. The backup tape does not allow you to access directory information.

You do not need to format tapes for a backup. However, before you perform a backup, make sure:

- your tapes are not write-protected
- you have enough tapes for the backup
- you loaded the tapes in the correct order

Note	You may need to maximize your browser window to see the entire **Tape Backup** screen.

To create a new backup job:

1. Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Tape Backup**.
2. Click **Create a new job** and enter a name for the job.
3. Select the volume(s) you want to back up.

4 Select a backup type. Click

- **Full Backup** to back up all the files in the selected volume(s).
- **Differential Backup** to back up only those files that have changed since the last full backup.

5 If you want to schedule the job, select the days you want to run the job. On the Tape Settings screen (see "Tape Settings" on page 5-21), you can change the scheduled start time. You can schedule only one job per day; however, several jobs can be configured to back up the same volume(s).

Note If you exit this screen without saving your changes, the modifications you made will be lost.

You can now:

- Save the job by clicking **Save**.
- Delete the job by clicking **Delete**.
- Modify the backup job.
- Run the backup job now.

For more information, see "Choosing Backup Options."

Choosing Backup Options

Note You may need to maximize your browser window to see the entire **Tape Backup** screen.

To run a backup job now:

1 Insert a tape or tapes into your Autoloader (make sure they are not write-protected). To verify that you loaded the tapes in the correct order, view the tape magazine (see "Tape Magazine" on page 5-13).

2 Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Tape Backup**.

3 Select an existing job from the drop-down list.

4 Select either **Run now, observe Tape Protection** to prevent tapes with recent data on them from being overwritten or **Run now, ignore Tape Protection** to disregard that setting.

5 Click **Run Job Now**. If you changed the backup schedule, a dialog box informs you that the job will be saved before the backup occurs. If you start a job using **Run Job Now** and a job is scheduled to run while your backup or restore is still in progress, the schedule job will not run. Click **OK** or **Cancel**.

6 The **Tape Backup Job Status** screen appears and displays the:

- Device Status
- Job Name
- Job Start Time
- Running Time
- Files and Bytes Processed
- Number of Tapes Accessed
- Bytes on Last Tape

Note You can also cancel the backup job.

7 When the job completes, view the tape log (see "Tape Log" on page 5-14) to determine which tapes were written to. This procedure is the only way to know which tapes were used (protected tapes may have been skipped). Remove those tapes from the Autoloader and label them.

To modify an existing backup job:

1 Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Tape Backup**.

2 Select an existing job from the drop-down list.

3 Modify the settings for the job.

4 Click **Save**.

To cancel a backup:

1 While a backup is in progress, click **Abort Running Job**.

2 Remove from the magazine any tapes that contain data you do not want to overwrite.

Note If you want to back up the same data from the canceled backup job, rename the checkpoint `backup.failed` to `backup`.

To delete a job:

1. Click the **Backup/Restore** tab, then select **Tape Backup**.
2. Select an existing job from the drop-down list.
3. Click **Delete**.

Backing Up Checkpoints

When a tape backup begins, it creates a checkpoint named `backup`. The information in the checkpoint `backup` is backed up to tape. If a checkpoint named `backup` already exists, that checkpoint is backed up instead.

Keep in mind:

- If the disk you are backing up is almost full, the attempt to create a backup checkpoint fails.
- If the backup completes successfully, the `backup` checkpoint is deleted.
- If the backup fails, the `backup` checkpoint is renamed `backup.failed` and is not deleted.

Note To control when data is frozen before being written to tape, you can rename any checkpoint (including `backup.failed`) to backup. Keep in mind that the renamed checkpoint is deleted when the backup completes.

Restoring Volumes, Files, and Directories

Restoring Overview

To restore a volume, file, or directory, you need to know which tape(s) the volume, file, or directory resides on and which tape drive slots the tape is loaded in. (Remember to always label your tapes.) In restoring files and directories, you must also know the full path of the file/directory that you are retrieving, starting with the volume name.

Caution If you start a restore and have a backup scheduled to occur after your restore finishes, the restore tape in the drive may be overwritten by the backup. To prevent this, remove the tape before the backup begins or write-protect the tape by sliding the write-protect switch until it clicks and an orange tab appears

The following information is retrieved from tapes that contain data:

- slot number being tested
- job on the tape
- position within the job
- date and time you last wrote data to the tape

If you are testing the *first* tape of the backup set, the following additional information is retrieved:

- a list of volumes on the tape
- type of backup on the tape (differential or full)

The first tape of a backup set must be selected to begin a restore.

Note If you changed the job since the backup, current information about the job may not reflect what is on the tape.

Restoring Volumes

Before you begin a whole-volume restore on disk:

- You might want to clear the volumes of current data because you will overwrite entire volumes.
- Make sure you restore from the full backup before restoring from a differential backup.

To restore a volume:

1. Insert the tapes containing the volume you want to restore in the Autoloader. Make sure you write-protect the tapes and load them in the correct order.
2. Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Tape Restore**.
3. To read the tape information, click on a tape icon below the tape's slot number. The following information about the tape appears on the screen for tapes that contain a backup:
   - slot number being tested
   - job on the tape
   - serial number of the tape
   - order of the tape within the job
   - type of backup performed (if it is the first tape of the backup)
   - date and time you last wrote data to the tape
   - volumes on the tape (if it is the first tape of the backup)

Note Loading and reading a tape takes at least three minutes.

4. Click **Restore Whole Volumes**.
5. A screen appears, listing the volumes on the tape. Select the volumes you want to restore.
6. Click **Start Restore**. A dialog box warning may inform you that if a backup is scheduled after you run a restore, the backup may overwrite your restore tapes. You should also write-protect your tapes or use the tape protection features on the **Settings** screen (see "Tape Settings" on page 5-21). Click **OK** or **Cancel**.
7. The **Drive and Job Status** screen displays the status of the restore. The screen refreshes every 10 seconds. To cancel the restore, click **Abort Running Job**.
8. When the restore is complete, view the tape log.

Note If the restore fails, make sure you view the tape log to determine what went wrong. For more information, see "Tape Log" on page 5-14.

Restoring Files and Directories

To restore a file or directory:

1. Insert the tapes you want to restore from in the Autoloader. Make sure you write-protect the tapes and load them in the correct order.
2. Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Tape Restore**.
3. To read the tape information, click on a tape icon below the tape's slot number. The following information about the tape appears on the screen for tapes that contain a backup:
   - slot number being tested
   - job on the tape
   - serial number of the tape
   - order of the tape within the job
   - type of backup performed (if it is the first tape of the backup)
   - date and time you last wrote data to the tape
   - volumes on the tape (if it is the first tape of the backup)

Note Loading and reading a tape takes at least three minutes.

4. Click **Restore Single File/Directory**.
5. A screen prompts you for the full path of the file(s) or directories you wish to restore. Make sure you use correct spelling and capitalization. Use forward slashes (/) between directories.
6. Select either:
   - Restore to original location
   - **Restore to directory on NetStorage 6000**. You must enter the destination path on the disk.
7. Click **Start Restore**. A dialog box warning may inform you that if a backup is scheduled after you run a restore, the backup may overwrite your restore tapes. You should write-protect your tapes or use the tape protection features on the **Settings** screen (see "Tape Settings" on page 5-21). Click **OK** or **Cancel**.
8. Before beginning a restore, the HP NetStorage 6000 searches the tape for the files. The **Drive and Job Status** screen displays the status of the restore. Check this screen periodically to see if the scan is successful.

The screen refreshes every 10 seconds. Even if you're restoring only a single file, the restore process might need to read through much of the backup set. To cancel the restore, click **Abort Running Job**.

9 When the restore is complete, view the tape log.

Note	If the restore fails, make sure you view the tape log to determine what went wrong. For more information, see "Tape Log" on page 5-14.

Checking Settings and Features

Tape Settings

The **Settings and Features** screen lets you:

- Change the start time for scheduled jobs.
- Change the number of days tapes are protected after backup.
- Tell the device which slot contains a cleaning tape.

Changing the Backup Schedule

Note	Scheduled jobs can have only one start time.

To change the scheduled start time for all backup jobs:

1 Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Tape Settings**.

2 Select the **Start time for scheduled jobs** field and enter a new start time using military format.

3 Click **Submit**. A dialog box informs you that you have changed the time for scheduled jobs. Click **OK**.

Changing the Tape Protection Window

The tape protection window is a *logical* write-protection mechanism that the server enforces. The window requires that you set the correct date and time on the server. You accomplish *physical* tape-protection with the write-protect tab on the tape cartridge. The tape protection window attempts to prevent accidental overwrite of tapes that are not physically write-protected.

The Autoloader tests each tape's protection setting before writing data to it. The default tape protection window is 7 days. For example, if a tape contains 5-day-old data and tape protection is 7 days, the Autoloader skips that tape and tests the next one. The Autoloader also skips write-protected tapes and cleaning tapes.

To change the protection setting for tapes:

1. Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Tape Settings**.
2. Select the **Backup tapes are protected from overwrite for** field and enter a new value.
3. Click **Submit**. A dialog box informs you that you have changed the number of days your tapes are protected. Click **OK**.

Skipping the Cleaning Tape

You can specify which slot contains a cleaning tape by skipping that slot during a backup or restore.

1. Using the NetStorage web interface, click the **Backup/Restore** tab, then select **Tape Settings**.
2. Click either:
   - **Use all tape magazine slots for backup and restore**.
   - **Slot** (specify slot) **contains a cleaning tape and will not be used for backup or restore**.
3. Click **Submit**.

Chapter 6
Monitoring the System

The Status Tab

The Status tab lets you:

- View status summary
- View event log
- View environmental parameters (temperature, voltages and cooling fan operation)
- View CPU utilization (both current and peak CPU values)
- View network transmission information (summary information on all Network Interface Cards in the system)
- View client activity on the network

Monitoring Hardware Information

Status Summary

Hardware status summary lets you view environmental and activity status. If an environmental item is running:

- out of specification, it is noted in the comment field and a hyperlink lets you access the corresponding page.
- within specification, a green light and an *ok* message are displayed.

To view hardware status summary:

Using the NetStorage web interface, click the **Status** tab, then select **Summary**.

The following information displays:

- Temperature problems link to **Environmental Monitoring** > **Air Temperature**.
- Power supplies. The five system voltages scanned and verified.

- Power modules. Informational messages about the power supply module status. If there are any error conditions, they are reported in the event log and any device notification systems that have been enabled.
- Cooling fans (on or off). Problems link to **Environmental Monitoring** > **Cooling Fans**.
- Network Transmission - NIC Port 1. The cumulative amount of packets in and out for the first or primary port since the machine was last reset or rebooted.
- Client Activity. Current number of clients attached to the HP NetStorage 6000.

Note The following symbols are used in the table:

— OK
— an item is critical
— the status information could not be obtained
— informational status only

View Event Log

You can view system messages two ways:

- **View Errors Only** displays only the error messages that have occurred in the system.
- **View All Messages** displays all messages that have occurred in the system. **Refresh** updates the view with the most recent event logging information.

To view the event log:

1. Using the NetStorage web interface, click the **Status** tab, then select **Event Log**. The following event information displays:
   - Date - mm/dd format
   - Time - 24 hour clock
   - Severity - (I = informational messages, E = error messages)
   - Description of event or error
2. Click:
   - **View Errors Only** to view error messages only.
   - **View All Messages** to return to the event log.
3. Click **Refresh** to update the log files.

You can use your browser's print command to print a copy of the log.

Note You can send a copy of the event log to a remote server. For more information, see "System Log" on page -9. Otherwise, the event log contains a fixed number of entries with the oldest item dropping off the log page. When the system is shutdown or rebooted the event log information is reset.

View Environmental Parameters

You can view hardware status graphically and numerically. The information is updated every 60 seconds. The following environmental systems are monitored and required for normal operation of the HP NetStorage 6000: temperature, power supply voltages, and cooling fans. See “Hardware Specifications” on page C-3 for more information.

To view environmental parameters:

1. Using the NetStorage web interface, click the **Status** tab, then select **Environmental Monitoring**.
2. Click on any of the three environmental systems to view its status.
   - **Air Temperature:** Two temperature gauges indicate the current air temperature in the HP NetStorage 6000 box. The temperature is displayed in degrees Celsius.
     A temperature error or failure is indicated in the status summary table if the temperature rises 15° C above the maximum ambient operating temperature of 40° C for more than 15 seconds.
   - **System Voltages:** The HP NetStorage 6000 has five system voltages that are monitored and maintained with three power supply modules (one is redundant). Five gauges display the current system voltage of each. If any voltage fluctuates by more than +/- 10% for more than 2 seconds it will be detected as an error and the appropriate notification and event log messages are sent.
   - **Cooling Fans:** Cooling fans maintain the necessary ambient temperature for maximum performance. The status of each fan is shown either as a:
     — black, spinning fan: fan is working normally
     — red fan: fan has failed.

Note	The RPM's of each fan are displayed beneath. Fans normally operate at or above 3750 RPM. A notification is posted on the status summary page and the event log if a fan has stopped or is not spinning at a high enough rate.

Caution	You must operate the HP NetStorage 6000 with the cover on. Otherwise, the fans will not cool the unit properly and it may overheat.

View CPU Utilization

CPU utilization lets you view the current load on the CPU of the HP NetStorage 6000. The information updates every 60 seconds. You can view the current load on the processor or the peak usage (the maximum load within the last five minutes).

To view the CPU Utilization:

Using the NetStorage web interface, click the **Status** tab, then select **CPU Utilization**. A CPU Usage chart appears displaying the current usage and the peak usage for the last five minutes.

Viewing System Activity

View Network Transmission Information

You can view network transmission information to see how much data is flowing across the network NIC ports in the HP NetStorage 6000. This information is used to determine if your network is running as efficiently as possible. If one of the NIC ports has too much traffic, you may want to move clients to another available NIC port. You can also view errors and collisions to spot potential hardware problems. The table is updated every five seconds.

To view network transmission information:

Using the NetStorage web interface, click the **Status** tab, then select **Network Transmission**. The following network transmission information displays:

- NIC name (Network Interface Card): This is automatically assigned by the HP NetStorage 6000.
- Network address (the network IP address): This is either assigned by the user or assigned using DHCP. If the port has not been configured, then <Not Configured> is displayed.
- Packets in: the cumulative total for this port
- Packets out: the cumulative total for this port
- Errors
- Collisions

Note This information is displayed separately for each NIC port even if you have taken advantage of port aggregation. When the HP NetStorage 6000 is reset or restarted, all of the numbers reset to zero.

View Client Activity

You can view client activity to see how many clients are currently attached to the HP NetStorage 6000 and the activity of the 20 most active clients. The most active client is listed at the top. The activity is defined as the total number of packets in and out for each client in the previous ten seconds. The client activity page updates every five seconds.

To view client activity:

1. Using the NetStorage web interface, click the **Status** tab, then select **Client Activity**.
2. The following information displays:
   - Client name - either an IP address or the system name
   - Total activity (packets in and out)

Note	The client's fully qualified name or their IP address displays depending upon the system's DNS configuration in settings.

Chapter 7
Reporting

The Report Tab

From the Report Tab you can send an HP NetStorage 6000 system information report to up to three e-mail addresses. This report provides information on hardware and software, file system configuration, NIC configuration, and environmental status. This report is helpful for checking configuration information as well as software and firmware versions.

Several attachments are sent along with this report such as the event log, the group and users map files, the `group.nis` file, the `password.nis` file, the `/etc/hosts file,` and the `/etc/approve` file.

To send a copy of this file and its attachments via e-mail:

1. Using the NetStorage web interface, click the **Reports** tab.
2. Enter the name of the e-mail server. The e-mail server must be an IP address or a fully qualified name (such as, alpha.corp.com).

Note If you change the e-mail server, it automatically changes the e-mail server specified on the SMTP/Email page. See “SMTP/Email” on page 3-7.

3. Enter the e-mail addresses of as many as three individuals. You must specify an e-mail server if one or more e-mail recipients are defined.
4. Click either:
   - **Send System Report Email** to send a report to the recipients and save your settings.
   - **Apply** to save your settings without sending a report.

Chapter 8
Securing Data

About HP NetStorage 6000 Security

This section explains the details of security as it applies to the user data stored on the HP NetStorage 6000. The NetStorage 6000 utilizes most of the security features found on Microsoft Windows, as well as all of the security features found on UNIX platforms. It is not the intent of this section to review the specifics of those security architectures. Instead, this section highlights the special features and differences that distinguish the security on the HP NetStorage 6000 from the security on traditional Windows or UNIX file servers.

Since the HP NetStorage 6000 is designed to serve files over both NFS and CIFS/SMB protocols, it is necessary to establish a mapping of the security architectures from one platform to the other. “Mapping NT and UNIX Users” on page 8-12 explains how that mapping is accomplished.

HP NetStorage 6000 Security in a UNIX-only Environment

The NetStorage 6000 utilizes an internal file system that is native to UNIX environments. As such, it has UNIX security mechanisms built-in that are leveraged when serving files over the NFS protocol. All resources stored on the file system contain the security metadata commonly found in UNIX systems.

The NetStorage 6000 does not support the concept of the `/etc/exports` file for managing mount points. Instead, the server automatically creates a single mount point at the root of all volumes created on the system. Since the server is specifically designed to share files, the exporting of mount points has been automated.

The root directory of the mount points on the NetStorage 6000 is given special permissions to facilitate appropriate access to users. The owner and group of this directory are root (UID = 0, GID = 0), and the permissions are read, write, and execute to owner, group and other (rwxrwxrwx). One

consequence of this setting is that all users can delete any file in the root of the mount point. Therefore, administrators are encouraged to avoid storing files in the root of the mount point.

The group assignment to files created in a file volume on UNIX can be performed in a variety of ways. On the NetStorage 6000, when a new file is created, the group assignment is inherited from the directory where the file is created. For example, if the group owner for directory `/acct/usr` is accountants (GID = 501), then all files created in that directory will be assigned a group owner of accountants (GID = 501).

Trusted Hosts

All UNIX clients that mount to file systems on the NetStorage 6000 use the UID and GID of their account when accessing files. A special case is the root user (UID = 0). In UNIX, the root user is a Super User, with full access to all files and directories in the file system. Due to the extensive rights provided to the root user, and the extensive damage that can be done by a malicious root user, the NetStorage 6000 does not trust them by default. Clients that attach with root privilege are given access as user **nobody** (UID = 60001), with no special rights or privileges.

The administrator can override this default behavior by declaring a particular client to be a Trusted Host. A root user mounting a NetStorage 6000 file system from a client that is a Trusted Host is given root privilege (UID = 0) to the file system. This feature allows administration of the file system by a root user, while at the same time, protecting the file system from other root users that should not have privileged access to the NetStorage 6000 file systems.

The administrator may declare Trusted Hosts using the web based administration tool, or the telnet administration tool of the NetStorage 6000.

The /etc Directory

It is necessary to maintain a number of system files on the NetStorage 6000 in an accessible place for administrative purposes. Some of the more common files found in this directory are:

Filename	Description
hosts	Resolves host names
hostgrps	Defines groups of host computers
approve	Restricts host access
users.map	Maps Windows user accounts to UNIX user accounts
group.map	Maps Windows group accounts to UNIX group accounts

All of these files are stored in the `/etc` directory on the first volume created on the system. The files in the `/etc` directory are for system management purposes and cannot be deleted. If the volume that stores the `/etc` directory is ever deleted, then the system moves the contents of this directory to another available volume.

Most of the files in the `/etc` directory may be edited through the web based user interface, or the telnet interface of the HP NetStorage 6000. In some cases, it is necessary to edit these files directly using a text editor. By default, all files in the `/etc` directory are owned by the root user, and may only be edited by the root user. Therefore, the only way to edit these files directly (using a text editor) is to mount the file system as the root user from a Trusted Host. See “Trusted Hosts” on page 8-2.

The /etc/approve File

Since the NetStorage 6000 does not support the `/etc/exports` file, support has been added for a file named `/etc/approve`. This file can be used to restrict NFS access to particular clients on the network.

In order to restrict individual clients and groups of clients to specific resources on the NetStorage server, the `/etc/approve` file must be edited. The file may be edited manually, or from the web based user interface, under the **Host Access** section of the Storage tab. Entries in the `/etc/approve` file have four fields. These fields are defined as follows:

Field	Description
class	This field specifies the class of object to protect. In all cases the object is **files**.
specifier	This field specifies the resources on the NetStorage 6000 server to protect. For example, **`/engineering`**, applies to all files and directories in the `/engineering` file system.
host pattern	This field has the name of a host or group of hosts that have access rights. Host names must be resolvable through the local `/etc/hosts` file, the NIS hosts file, or through DNS. Groups of hosts are specified in the `/etc/hostgrps` file. If the host pattern is the name of a group, then it must be preceded by the @ symbol. The wildcard character (*) may be used to specify all hosts.
rights	This field specifies the access limits to apply. The entry in this field can be one of the following: • **access=rw** allows read and write access to the resources • **access=ro** allows read only access to the resources • **access=none** denies all access to the resource

Additional information about the format of this file, as well as detailed examples may be found in “Edit Host Access” on page 4-15.

The file is searched sequentially for a match. Once an entry is found that matches the host and the resource to restrict, all other entries are ignored.

HP NetStorage 6000 Security in an NT-only Environment

On Microsoft Windows, the protocol used to transfer files over the network between a server and a client is known as Server Message Block (SMB), or Common Internet File System (CIFS). Many variations of the protocol exist which reflect the myriad flavors of Windows on the Market; Windows 95/98, Windows NT, and Windows 2000.

Given all these variations, there are two distinct mechanisms used in CIFS to provide security for resources. They are known as Share-Level Security and User-Level Security. The HP NetStorage 6000 supports both of these security modes. The next two sections briefly explain the architecture of these security modes, and highlight any special considerations that should be noted for the HP NetStorage 6000.

Share-Level Security

Share-level security is the simplest CIFS security mode to use, but offers the least security. In this mode, each share is protected by a password. When the server administrator defines a new share, a password is specified to protect the share from unauthorized access. When a user first accesses the share they are prompted for the password. Once the password is entered and verified, then the user has full access to all files on the share. Share-Level security is the default security mode for Windows for Workgroups and Windows 95.

Share-Level security may be implemented to allow both Read/Write access, as well as Read Only access to shares. Each share may be protected by a Read/Write password and a Read Only password. The access allowed on the share (Read/Write or Read Only) is dictated by the password entered by the user.

By default, the NetStorage 6000 accepts encrypted passwords for verification. In these cases, Windows NT (also known as NT LM 0.12) password encryption is used. The NetStorage 6000 also accepts plaintext passwords from older clients, for backward compatibility.

Since the native file system on the NetStorage 6000 is UNIX based, all files must have a UID and GID associated with them. However, since Share-Level security does not support the concept of users or groups, a single UID and GID is assigned to each share, such that all files created in the share from Windows clients are assigned the UID and GID of the share. When shares are managed through the web based administration tool, shares are automatically assigned a UID and GID of zero (UID = 0, GID = 0). For administrators with special needs, the default UID and GID of zero may be changed for a given share. The telnet interface of the NetStorage 6000 allows the user to specify the UID and the GID to be used for a particular share. In this case, ALL directories and files created in the share are assigned the UID and GID specified by the administrator.

Since Share-Level security allows the user full access to all files regardless of the UNIX permission settings, it is up to the administrator to ensure that the Windows shares are created in such places so as not to expose sensitive system files, or the resources of other UNIX users.

User-Level Security

User-Level Security offers superior flexibility and ease of use on networks with a significant number of users and/or resources. In this mode, each user provides their logon account credentials to gain access to a computer or network rather than providing passwords for network shares. Using this method of security resources can be protected either at share, directory or file level. Each resource may be protected on a user by user basis that allows almost infinite permutations of access restrictions of users and groups of users. User-Level Security is the default security mode of Windows NT systems.

The user accounts may be either local machine accounts for access to a single computer, or they may be accounts that apply to all computers attached to the network. If a computer is attached to a network, then local machine accounts are of little value, since the user of that account may only access resources on that computer, and not any other computer on the network. On the other hand, network-wide accounts allow users to access resources on other computers on the network. In addition, these accounts allow the user to logon to any computer on the network.

On NT networks, the network wide user accounts are managed through NT domains.

Under User-Level security, each computer on the network is responsible for authenticating users before the user is allowed to access the resources on that computer. Once a user is authenticated on a computer, a session is established with the user. The user does not need to be authenticated again during that session. This not only applies to users accessing machines directly (interactive logon), but also to users accessing resources on remote servers (remote, or network logon).

Interactive logon is a very common experience for most users. Every time a Windows NT computer boots, a user must logon to the system before gaining access to any resource. The user is prompted to press Ctrl-Alt-Del and then enter a name, password and NT Domain name at the console of the local computer. Once the user is authenticated with these credentials, the user is allowed access to the resources of the computer.

Remote logon is not as obvious to most users. When a user attempts to access files on a remote computer (such as through Network Neighborhood, or by mapping a network drive to a drive letter), the remote computer must first authenticate the user before allowing access, even though the user has already logged onto the local system. Unlike the

interactive logon, remote logon usually occurs automatically, without user interaction. The local computer offers the account name and password from the interactive logon as credentials to logon to the remote computer.

The HP NetStorage 6000 fully supports the remote logon process. There is no distinction between how the HP NetStorage 6000 authenticates users and how a Windows NT 4.0 server authenticates users. However, since the HP NetStorage 6000 does not offer a local console interface, interactive logon is not supported. In addition, user and group accounts local to the HP NetStorage 6000 are not supported. In User-Level security, access is only allowed to users in a Windows NT domain environment.

The HP NetStorage 6000 currently does not support authentication through Windows 2000 domain controllers running in native mode. The HP NetStorage 6000 also does not participate in the Windows 2000 Active Directory Services (ADS). However, the HP NetStorage 6000 can authenticate through a Windows 2000 domain controller operating in mixed mode. This means that the domain controller is configured to authenticate Windows NT 4.0 style requests in addition to native Windows 2000 style requests.

Security Descriptors

Windows NT, in conjunction with the NT File System (NTFS), is designed to support restricted access to any object (i.e. files or directories) on the File System. Every file and directory stored on the system contains a small amount of administrative information (often referred to as metadata), which includes the security information associated with the object. This information is known as the Security Descriptor, and contains the following main attributes:

Attribute	Description
Owner SID	The owner's security ID
Group SID	The security ID of the primary group for the object (used only by POSIX)
Discretionary Access Control List (DACL)	Specifies who has what access to an object
System Access Control List (SACL)	Controls the auditing messages the system will generate. System ACLs are controlled by the administrators.

This security mechanism protects the object from unauthorized access, regardless of whether the user attempts to access the object on the local machine, or over the network from a client system.

The Discretionary Access Control List (DACL), is by far the most common form of access control list, and is often abbreviated simply as the ACL of an object. The ACL is what is used to establish a security policy on every file and directory within a file system. Using this mechanism, users can restrict access to objects from other users or groups of users.

Although the HP NetStorage 6000 does not use the NTFS file system as it's local file system, it does support having NT Security Descriptors for every object in the file system. Thus, users can set security policies for files and directories as though the file system were NTFS.

By default, all files and directories created via the NFS protocol (from a UNIX or Linux client) do not contain security descriptors. Such files are known as UNIX files. All files and directories that are created from Windows clients, or UNIX files that are modified from a Windows client, are automatically assigned a security descriptor. Files and directories that have security descriptors are known as Windows files. The main functional distinction between UNIX files and Windows files is that UNIX users cannot change the ownership (chown) or permissions (chmod) of Windows files.

Security Mapping in a Heterogeneous Environment

The HP NetStorage 6000 works in a heterogeneous environment and supports remote file access protocols for both UNIX-based and NT-based clients. A major difficulty in sharing data across these two environments is that the file system security is different. NT systems that use user-level security use ACLs to identify both themselves and the permissions for each data object, whereas UNIX systems use traditional UNIX permissions that define explicit permissions for the user, group, and other. A reasonable level of access can be provided for cross-environment requests (i.e., UNIX requesting NT files) without compromising the security set by the creator of the object. The rule is that a client can never be granted greater access than the client would have been granted in the environment where the object was created.

With the HP NetStorage 6000 in User-Level security, you can enable a mapping function that allows clients to access file resources in either UNIX or Windows environments with the same security permissions. An NT client, when attaching to the HP NetStorage 6000 for the first time where user-level security is being used, has a UID and GID automatically generated and stored in the users map file. The UID and GID values uniquely identify the user as a member of a specific domain. Any objects that are created or modified have a security descriptor attached to them that contains information about their unique identity. If you explicitly provide a security descriptor when creating an object, that is associated with the object. If you do not specify security for the object, then the directory in which the object resides is consulted for inheritable ACLs to form the new security descriptor. If neither of the conditions applies, then the object has a default ACL.

UNIX Files Accessed by NT Clients

When an NT user accesses a UNIX file, the UNIX file permissions are translated into an ACL that then determines the permissions to grant. Recall from "HP NetStorage 6000 Security in a UNIX-only Environment" on page 8-1 that permissions are granted to three distinct groups:

- user
- group
- other

If the owner of the UNIX file does not map to a user in the NT domain, then an NT user ID is generated in the local UNIX domain. If the owner of the UNIX file is recognized (or mapped) as a known NT user, then the appropriate information is exchanged so that the owner has the same security privileges in NT as in UNIX. A similar process occurs for the group identification and permissions. The **Other** field is mapped to the NT **Everyone** account. The table below shows the mapping that takes place between the permissions in UNIX and NT.

UNIX	NT Equivalent
r--	Read
-w-	Write, Delete
--x	Execute
-wx	Write, Delete, Execute
r-x	Read, Execute
rw-	Read, Write, Delete
rwx	Full Access
---	No Access

Note If the UNIX file is modified by an NT client, then the file becomes an NT file.

NT Files Accessed by UNIX Clients

Directly mapping NT permissions to UNIX permissions causes some difficulty because NT permissions have a greater level of complexity. UNIX users are unable to use either the **chmod** or **chown** commands to modify the permissions or owners of NT files. The table below shows which UNIX-to-NT file permissions are mapped.

NT File or Directory	UNIX File or Directory
R	r
W	w
X	x
D	ignored
P	denied
O	denied

In addition to the permission mappings covered in the previous sections, the following also applies:

- If no ACLs are specified, then the UNIX permission is `rwxrwxrwx`.
- If the ACL is empty, then the UNIX permissions will be `----------`.
- If the only access allowed by the ACL grants full control to everyone, then the UNIX permissions will be `rwxrwxrwx`.
- In the absence of a group ACL, the owning group will be the user's primary group and the group permissions are set to the same value as the other permissions.

Additionally, if an NT file grants permission to the Everyone group (and does not specifically deny access to the owner or the group), then the same access is given to the owner and the primary group. However, UNIX permissions look for explicit permissions for the owner, group, and other. To allow the same level of access in UNIX as NT, these files will have a permission of `r--r--r--`.

Mapping NT and UNIX Users

If you have clients with NT and UNIX accounts, and you select user-level security, you need to ensure that these clients have the same file access and security regardless of the environment that they choose to work in. Similarly, you might want to make either UNIX or NT files available to clients in other environments. To accomplish this task, you need to create a mapping between your users and groups. See “Mapping Strategy” on page 3-14. The following table helps you determine how to go about this task.

Environment	Suggested Action
NT users do not want access to UNIX files and UNIX users do not want access to NT files.	No mapping required.
Homogenous UNIX environment. Only UNIX files will be stored on the HP NetStorage 6000.	No mapping required.
Homogenous NT environment. Only NT files will be stored on the HP NetStorage 6000.	No mapping required.
Clients want to share files across UNIX and NT environments. NT user names are identical to UNIX user names.	Use **User Name Mapping**. In attempting to match UNIX and NT user names, the HP NetStorage 6000 consults the `passwd.nis` file for UNIX user names and user IDs and then attempts to match the name with the NT user name.

Environment	Suggested Action
NT user's full name is identical to the UNIX comment field.	Use **Full Name Mapping**. In attempting to match the UNIX comment field and NT user's full name, the HP NetStorage 6000 consults the `passwd.nis` file for the UNIX comment field and user ID and compares this with the NT user full name field.
NT group names are identical to the UNIX group names.	Use **Group Name Mapping**. In attempting to match the UNIX group names and NT group names, the HP NetStorage 6000 consults the `group.nis` file for the UNIX group names and their IDs and compares this with the NT group name field.

Note The HP NetStorage 6000 does *not* authenticate UNIX accounts and thus does not use the security files from NIS for authentication or account name resolution. The only reason to store and maintain these files is to map UNIX users to NT users. If the server is not used for NT access, or if the storage for NT users and the storage for UNIX users are kept separate, then there is no need to maintain these files.

Modifying Map Files

The mapping files that are created by the HP NetStorage 6000 for users (user map) and groups (group map) can be manually edited if necessary. You might consider manually modifying the files for any of the following reasons:

- If an incorrect association has been made between two clients (NT to UNIX).
- If you remove a client as part of a file cleanup.
- If you create custom associations between users.

The user map and group map files are located in the `/etc` directory at the root of the first volume. But you can modify the user map file and group map file through the NetStorage web-based interface. See "Modifying the User Map File" on page 3-19 and "Modifying the Group Map File" on page 3-20.

User Map File

If the administrator has chosen No Mapping, the first time an NT client attaches to the NetStorage 6000, an entry is made in the user map file that includes the client's NT username, NT domain, NT RID, and an *assigned* UID and UNIX username. The user map file entries have the following format:

```
<UNIX username>:<UID>:<NT username>:<NT domain>:<NT RID>
```

To ensure uniqueness, the UID that is assigned is a number one greater than any UID value found in the users.nis or users.map file. The assigned username is the UID preceded by **u**. For instance, if the UID is 502, the username is u502.

Group Map File

If the administrator has chosen No Mapping, the first time an NT client attaches to the NetStorage 6000, the primary group for the NT client is obtained and added to the group map file in addition to an *assigned* GID and UNIX groupname. If the primary group for this client is already present in the group map file, no changes are made. The group map file entries have the following format:

```
<UNIX groupname>:<GID>:<NT groupname>:<NT domain>:<NT RID>
```

To ensure uniqueness, the GID that is assigned is a number one greater than any GID value found in the group.nis or group map file. The assigned groupname is the GID preceded by **g**. For instance, if the GID is 21, the groupname is G21.

Modifying Files

Since NIS files are read-only, the only files that can be modified are the user map and group map files. The fields you can edit are:

Field	Restrictions
username	Any combination of letters and numbers up to 256 characters. This must be a unique value in the user map file.
UID	This numeric-only entry must be unique in the user map file.
groupname	Any combination of letters and numbers up to 256 characters. This must be a unique value in the group map file.
GID	This numeric-only entry must be unique in the group map file.

Note Use care when modifying these files to be sure that the names and domains are correctly spelled. Otherwise, your clients might experience some unexpected results.

Chapter 9
Contacting Support and Upgrading

The Support Tab

The support tab lets you:

- Contact service and support for the HP NetStorage 6000
- Register the HP NetStorage 6000
- Upgrade the HP NetStorage 6000

HP NetStorage 6000 Service and Support

HP's electronic services give you a fast, interactive way to access information and help about setup, configuration, installation, and operation of your product.

To access HP Service and Support:

Using the NetStorage web interface, click the **Support** tab, then select **Contact Information > Contact Details**.

You can choose to:

- Visit the HP website by clicking on **HP NetStorage 6000 Support Website**.
- Send e-mail to customer support by clicking on **Send e-mail to HP Support**.
- Obtain the HP Customer Support phone number.
- Purchase additional NetStorage hardware and upgrades through the HP Business Store by clicking on **Buy Online**.

Registering the HP NetStorage 6000

When you register your HP NetStorage 6000, you receive important information on the latest upgrades directly from HP.

To register your HP NetStorage 6000 online:

1. Using the NetStorage web interface, click the **Support** tab.
2. Select **Contact Information** > **Register via the Web**.
3. Click **Register at HP.COM web site** and follow the instructions.

To register through HP Customer Support:

Call HP Customer Support at (970) 635-1000.

Note After registering your unit, you can use the **Support** tab to upgrade the system when upgrades are available.

Upgrading the HP NetStorage 6000

Upgrade Overview

Note You must register your HP NetStorage 6000 before you can receive upgrade information. See “Registering the HP NetStorage 6000” on page 9-2.

You should periodically ensure that you have the latest operating system, user interface, and documentation on your system. The HP NetStorage 6000 operating system software connects to the hp.com web site and runs a script to see if newer files exist.

Note If your network is located behind a firewall, you may need to configure your web browser with a proxy to connect to the hp.com web site in order to check your configuration or download an upgrade.

To obtain an upgrade:

1. Using the NetStorage web interface, click the **Support** tab, then select **Upgrades > Check My Configuration**. A screen displays:
   - The version number of the software you are running.
   - Whether a newer version is available.
2. If you:
   - Are running the latest version of the software, click **Back** or **Cancel**.
   - Want to upgrade, click **Proceed to Download Page** and follow the directions on screen.

To complete a successful upgrade, you must:

1. Obtain a copy of the operating system upgrade by downloading the latest operating system, user interface, and documentation. For more information, see “Upgrading From the Web” on page 9-4.
2. Upload the upgrade to the HP NetStorage 6000.
3. Reboot the HP NetStorage 6000 to activate the upgraded software.

Note To delay the installation of the upgrade, you can download the file and install it later. For more information, see “Upgrading From Downloaded File” on page 9-5.

Upgrading From the Web

Note You must register your HP NetStorage 6000 before you can upgrade. See "Registering the HP NetStorage 6000" on page 9-2.

To upgrade from the web:

1. Using the NetStorage web interface, click the **Support** tab, then select **Upgrades > Start Upgrade Now**.
2. Click **Download it from the HP website**, then click **Next**. An upgrade screen appears, listing the:
   - Version number of your software.
   - Status of the software (which version you are currently running and which version is the latest available).
   - Date the software is available.
   - **Details** button you can click to obtain more information about the version of the software.
   - A brief description of the version.
3. If you are running the latest version of the software, click **Back** or **Cancel**.
4. If you want to upgrade:
   a. Click the radio button next to the software version you want to download.
   b. Click **Start Download**.
   c. In the FTP window, either open the downloaded file from its current location or select where to save the file.
   d. Click **OK**.

Note At this point, the upgrade file resides on your local drive, *not* on the NetStorage device. You can either continue with the upgrade now or do so at another time by quitting now, then selecting **It's on my file system already** when you are ready to upgrade.

5. A screen prompts you for the location of the upgrade file. Enter the path of the upgrade file or click **Browse** to locate it. You can also enter a description or comment to help you easily identify the file.
6. Click **Upload Image to NetStorage 6000**.

7 After your system uploads the image to the HP NetStorage 6000, you must reboot the device in order for the upgrade to take effect. You can click either **Reboot Now** (if the reboot won't interrupt the operation of your network), then click **Finish** or you can select **Reboot Later**.

Upgrading From Downloaded File

If you already downloaded the file:

1 Using the NetStorage web interface, click the **Support** tab, then select **Upgrades > Start Upgrade Now**.

2 Click **It's on my computer's File System Already**, then click **Next**. For more information, see "Upgrading From Downloaded File" on page 9-5.

3 A screen appears, asking you to specify where you downloaded the upgrade file. Enter the path of the upgrade file or click **Browse** to locate it.

4 Click **Upload Image to NetStorage 6000**.

5 After your system uploads the image to the HP NetStorage 6000, you must reboot the device in order for the upgrade to take effect. You can click either **Reboot Now** (if the reboot won't interrupt the operation of your network), then click **Finish** or you can select **Reboot Later**.

Chapter 10

Integrating with Management Applications

Management Applications Overview

HP TopTools

HP TopTools is a tool for managing devices on a network. It discovers the devices on your network and maintains information about their configuration and status. This information is stored on a web server. You access the device information using a web browser.

HP TopTools version 5.0 has built-in support for the HP NetStorage 6000. HP TopTools version 4.5 for Windows NT may be used, but it does require a software update.

Network Management Applications

The HP NetStorage 6000 integrates with the following network management applications:

- HP OpenView Network Node Manager version 6.0 and 6.1
- Computer Associates (CA) Unicenter TNG Framework version 2.2

The integration allows each network management application to:

- Identify the HP NetStorage 6000 when it is attached to the network.
- Display the HP NetStorage 6000 icon in the platform's network topology map.
- Launch the HP NetStorage 6000 web-based user interface from pop-up menu.
- Receive and process event notifications from the HP NetStorage 6000.

The following network management applications are supported:

- HP OpenView Network Node Manager version 6.0 for Windows NT and UNIX
- CA Unicenter TNG Framework version 2.2 for Windows NT and UNIX

To install the HP Network Management Integration Packs refer to the installation poster and *HP NetStorage 6000* CD that came with your unit.

Note	For detailed information about the NetStorage 6000 in OpenView, open the SNMP MIB browser and navigate to the following path: iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).hp(11).nm(2).system(3).netperipheral(9).hpnetworkstorage(12).ns6000(1).ns6000_1(1).ns6000MIB(2)

System Management Tools

HP OpenView ManageX is the Application and System Management component of the Windows NT Management tool, named HP OpenView Express.

The HP NetStorage integration allows:

- HP NetStorage 6000 events to be monitored by HP OpenView ManageX.
- ManageX Message Reader to receive and display event notifications from the NetStorage 6000.
- Links to the HP NetStorage 6000 web-based management page from the ManageX console.

HP Top Tools Integration

Note	The integration pack must be installed on the machine running HP TopTools.

To install HP Top Tools:

1. Close all HP TopTools program pages.
2. From the Control Panel, select **Services**.
   a. Stop the **HP TopTools Services**. If this fails, set the startup mode to Manual, reboot and go to step b.
   b. Stop the **IIS Admin Service**. Click **OK** on the dialog box that lists the WWW Publishing Services.
3. Insert the *HP NetStorage 6000* CD into your CD-ROM drive.
4. Run the following program and follow the screen instructions.
   `\TopTools\WinNT\setup.exe`
5. From the Control Panel, select **Services**.
   a. Restart **WWW Services**.
   b. Restart **HP TopTools Services**.
6. Open the HP TopTools main page.
   - If prior to running the integration pack, TopTools has already detected the HP NetStorage 6000 device:
     a. Locate the HP NetStorage 6000 device. They will be listed by the name you have specified.
     b. Right-click on the device.
     c. In the pop-up menu, select **Update Discovery**.
   - If TopTools has not already detected the device, run Discovery from HP TopTools by selecting **Settings** > **Discovery user interface**.

To uninstall the integration pack:

The integration pack cannot be removed.

HP OpenView Network Node Manager Integration

Windows NT Installation

Note	You need to be at the Windows NT server or workstation where HP OpenView is installed.

To install HP OpenView NNM for Windows NT:

1. Make sure that Network Node Manager (NNM) Services has been started.
2. Shut down the NNM graphical user interface program.
3. Insert the *HP NetStorage 6000* CD into your CD-ROM drive.
4. Run the following program and follow the screen instructions. The **Finish** dialog box appears when the installation is complete.

   ```
   \Ovw\WinNT\setup.exe.
   ```

5. Start the NNM graphical user interface program. The HP NetStorage 6000 symbol and menu do not appear until NNM discovers it at the next polling time.

You may see the following error appear when running the NNM program the first time. This error should disappear in subsequent runs of NNM.

```
0:46:42 ovw (0xA82):
-----------------------------
File: C:\OpenView\symbols\C\Server\Server_hpns6000
Line: 6
Error: Unknown field "isHPNS6000"
-----------------------------
10:46:44 ovw (0xA82):
-----------------------------
File: C:\OpenView\registration\C\hp_6k\hpns6Kapp
Line: 37
Error: Unknown field "isHPNS6000"
-----------------------------
```

To uninstall the integration pack:

1. From the Windows control panel, select **Add/Remove Programs**.
2. Select the **NNM-NetStorage 6000 Integration Pack**, then click **Add/Remove**.

UNIX (HP-UX and Sun Solaris) Installation

Note You need to be at the HP-UX or Solaris machine where HP OpenView is installed.

To install HP OpenView NNM for UNIX:

1. Make sure that Network Node Manager (NNM) Services has been started.
2. Shut down the NNM graphical user interface program.
3. Insert the *HP NetStorage 6000* CD into your CD-ROM drive.
4. Run the following script `/ovw/HPUX_Sol/install.sh` by typing

```
cd /cdrom
cd /ovw/HPUX_Sol
/install.sh
```

5. Start the NNM graphical user interface program. The HP NetStorage 6000 symbol and menu will not appear until NNM discovers it at the next polling time.

To mount the HP-UX CD-ROM:

Note The CD can be read correctly only with a pfs_mount CD-ROM command.

1. At the console, start the following background processes (& = background process):

```
> pfs_mountd&
> pfsd&
```

2. Verify such background processes exist with:

```
> ps -ef | grep pfs
```

3. At the console, enter:

```
> pfs_mount /cdrom
```

or

```
> pfs_mount <device-file> /cdrom
```

(an example of <device-file> is /dev/dsk/c1t2d0 ; i.e., > pfs_mount /dev/dsk/c1t2d0 /cdrom)

4. Verify the CD-ROM is mounted by entering

```
> bdf
```

5. When finished, unmount the CD-ROM with the command:

```
> pfs_umount /cdrom
```

To uninstall the integration pack:

1 Go to the directory where the `uninstall.sh` file resides.

```
Cd "$OV_BIN/HP_NS6000
```

2 Run the `uninstall.sh` file by entering:

```
./uninstall.sh
```

The following message may appear if NNM has not discovered a HP NetStorage 6000 box in its network prior to the integration setup.

```
No nodes were found with sysobjid
1.3.6.1.4.1.11.2.3.9.12.1.1
```

You may ignore this message.

CA Unicenter TNG Framework Integration

Windows NT Installation

Note	The integration pack must be installed on the machine running Unicenter Framework.

To install CA Unicenter TNG Framework for Windows NT:

1. Shut down any Unicenter programs that are currently running.
2. Insert the *HP NetStorage 6000* CD into your CD-ROM drive.
3. Run the following program and follow the screen instructions:

   ```
   \CA_Frmwk\WinNT\setup.exe
   ```

4. A **Finish** dialog box appears when the installation is complete. Click **OK**.
5. Select **Start > Programs > Unicenter TNG Framework > Auto Discovery** to start the Unicenter Auto-Discovery process.
6. Select **Start > Programs > Unicenter TNG Framework > 2-D MAP** to open the Unicenter 2-D map to view the HP NetStorage 6000 icon.
7. Select **Start > Programs > Unicenter TNG Framework > Enterprise Managers > Windows NT > Event > Console Logs** to open the Unicenter Enterprise Management console to view the HP NetStorage 6000 traps.

Known Issues

If you run an Auto-Discovery before installing the HP NetStorage 6000 integration pack, the HP NetStorage 6000 will show up under one of two areas:

- If it appears as an *Unclassified* device:
  a. Right-click on the device, select **Reclassify**.
  b. When the **Edit Class** notebook appears, select **OK**.
- If it appears as an *Other Device*:
  a. Right-click on the device, select **Delete Object**.
  b. Click **OK**.
  c. Run an Auto-Discovery.

When receiving a trap in the console log, a message highlighted in red appears. Additionally, the icon in the 2-D map should change colors.

If the icon does not change colors, you must:

1. Select **Start > Programs > Unicenter TNG Framework > Enterprise Managers > Windows NT > Configuration > Settings**.
2. On the bottom tab click on **Event Management**. Click **Client Preferences** on the right hand tab.
3. Look for the `Users authorized to issue commands entry`. In the settings area enter `[machine name]\caunint,caunint`.

To uninstall the integration pack:

1. From the Windows control panel, select **Add/Remove Programs**.
2. Select the **TNG Framework NetStorage 6000 Integration Pack**, then click **Add/Remove**.

HP-UX or Sun Solaris Installation

Note The integration pack must be installed on the machine running Unicenter Framework.

To install CA Unicenter TNG Framework:

1. Shut down any Unicenter programs that are currently running.
2. Insert the *HP NetStorage 6000* CD into your CD-ROM drive.
3. Go to the `/Ca_Frmwk/HPUX_Sol` folder by typing

   ```
   cd /cdrom
   cd Ca_Frmwk/HPUX_Sol
   ```
4. Locate the `install.sh` file on the CD (`/CA_Frmwk/HPUX_Sol/`).
5. Run the `install.sh` file by typing `./install.sh`.
6. Start the Unicenter Auto-Discovery process.
7. Open the Unicenter 2-D map to view the HP NetStorage 6000 icon.
8. Open the Unicenter Enterprise Management console to view the HP NetStorage 6000 trap messages.

Known Issues

If you are logging into the UNIX box remotely, you may not use the Manage HP NetStorage 6000 or the Reset HP NetStorage 6000 menu items. To access the HP NetStorage, you must:

1. Open up the web browser on the machine you are using.
2. In the URL, type in the IP address of the HP NetStorage 6000.

To mount the HP-UX CDROM:

Note The CD can be read correctly only with a `pfs_mount-ed` CD-ROM command.

1. At the console, start the following background processes

```
(& = background process):
 > pfs_mountd&
 > pfsd&
```

2. Verify such background processes exist with:

```
> ps -ef | grep pfs
```

3. At the console, enter:

```
> pfs_mount /cdrom
```

or

```
> pfs_mount <device-file> /cdrom
```

4. Verify the CD-ROM is mounted by entering:

```
> bdf
```

5. When finished, unmount the CD-ROM with the command:

```
> pfs_umount /cdrom
```

To uninstall the integration pack:

1. Go to the directory where the `unistall.sh` files resides by typing

```
cd "$CAIGLBL0000/hpns6000"
```

2. Run the uninstall.sh file by entering:

```
./uninstall.sh
```

3. Restart the NetView user interface. The next time NetView discovers the HP NetStorage 6000 device, it is properly represented on your map.

- If the HP NetStorage 6000 trap definitions do not load into NetView, then the NetView environment is not in setup in the specified location. The path to the NetView executables must be in the system path environment variable.

ManageX Integration

The ManageX and HP NetStorage 6000 integration pack provides a means for ManageX to detect operational problems with the HP NetStorage 6000. It utilizes the Web-based Enterprise Management (WBEM) support capability of ManageX. The HP NetStorage 6000 can send its traps to the ManageX message reader for event management. The system administrator can go to the HP NetStorage 6000 web-based management page directly from the ManageX console. The system administrator is notified immediately of problem events, such as RAID disk drive failure or space over-utilization.

The trap notification uses SNMP and Windows Management Instrumentation (WMI). WMI is the Microsoft implementation of the WBEM technology, which ManageX supports. The HP NetStorage 6000 integration includes:

- WBEM policy designed to forward HP NetStorage 6000 enterprise-specific traps to ManageX.
- Capability to open the HP NetStorage 6000 management page in the Microsoft Management Console (MMC) along with ManageX

Adding the HP NetStorage 6000 URL snap in:

To have the URL of the HP NetStorage 6000 web-based management page inserted in the console tree of the ManageX Console Root:

1. Start ManageX.
2. From the MMC window menu drop-down list, select a window having Console Root. If no such window exists, click on **Window > New Window**.
3. From the main MMC window menu, select the **Console** pull-down menu.
4. Select **Add/Remove Snap-in**. The **Add/Remove Snap-in** dialog box appears.
5. Click **Add**. The **Add Standalone Snap-in** dialog box appears.
6. With **Folder** highlighted, click **Add** then **Close**. The **Add/Remove Snap-in** dialog box now has a new folder in it. Click **OK**.
7. Rename the **New Folder** to **HP NetStorage Administration** by right-clicking on **New Folder** and selecting **Rename**.

To install the WMI event policy:

1. On ***SYSTEMWMI*** install and start the Microsoft WMI Core service. The WMI Core installation file, `wbemcore.exe`, is located on the ManageX program CD in the `\Redist\x86\Li\` directory.
2. Install and start the Microsoft WBEM SNMP Provider service. The WBEM SNMP Provider installation file, `wbemsnmp.exe`, is located on the ManageX program CD in the `\Redist\x86\Li\` directory.
3. On ***SYSTEMMANAGEX***, find the directory name where HP OpenView ManageX policies have been installed on the Windows NT system. The default location is `C:\Program Files\HP OpenView ManageX\Policies\`.
4. In this directory, create a folder named HP NetStorage (for example, `C:\Program Files\HP OpenView ManageX\Policies\HP NetStorage\`).
5. Copy `HPNetStorage6000Events.mxw` to this folder.
6. Start ManageX and expand or open the Policies snap-in in the ManageX console's left pane.
7. Select **Available** then **HP NetStorage**. You see the new policy, HP NetStorage 6000 WMI Event, in the right pane. If ManageX is already running you can select **Refresh** from the context menu by right-clicking on **Available** under the Policies snap-in.
8. Open the Device Selector dialog box (right-click on **OpenView ManageX** and chose **Device Selector**) and select the ***SYSTEMWMI*** computer.
9. Use the normal policy deployment mechanism in ManageX and install the HP NetStorage 6000 WMI Event Policy to the ***SYSTEMWMI*** computer. Make sure that ***SYSTEMMANAGEX*** session is logged in to the network domain, not the local ***SYSTEMMANAGEX*** domain. This is necessary in order to deploy a policy to the ***SYSTEMWMI*** computer.

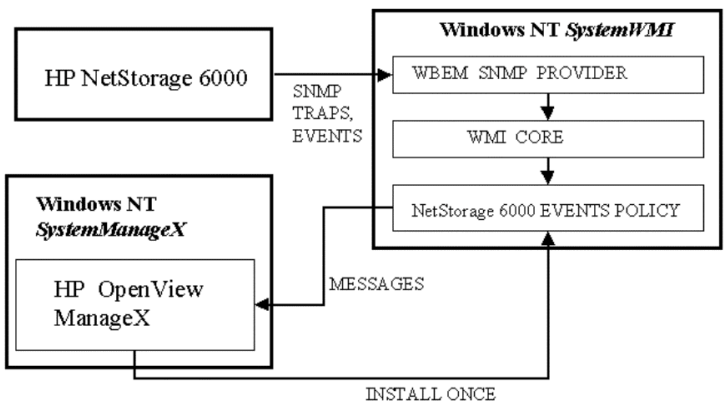
Setting up HP NetStorage 6000 SNMP Alerts

From an HTML browser, open the main web-based user interface page for the HP NetStorage 6000 that you want to monitor. The URL of the selected NetStorage 6000 main page is either its mapped network name or its IP address.

To set up the SNMP alerts:

1. In the NetStorage web interface, click the **Configuration** tab, then select **Alert Settings > SNMP/Network Management**.
2. Enter the IP address of the ***SYSTEMWMI*** computer in one of the unused **Trap Destination** fields, or change an existing field to the IP address of ***SYSTEMWMI*** computer.
3. Click **Apply**.

Figure 10.1 HP NetStorage 6000 Trap Route View



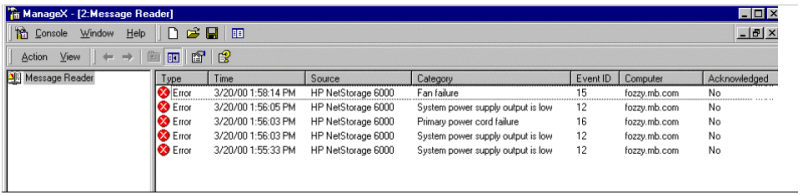
Viewing the ManageX Message Reader

The example in figure 10.2 shows how HP NetStorage events are presented in the ManageX message reader.

To view this window:

In the left pane, select **OpenView ManageX > Message Reader**.

Figure 10.2 The ManageX Message Reader


ManageX - [2:Message Reader]
Console Window Help
Action View
Message Reader
Type Time Source Category Event ID Computer Acknowledged
Error 3/20/00 1:58:14 PM HP NetStorage 6000 Fan failure 15 fozzy.mb.com No
Error 3/20/00 1:56:05 PM HP NetStorage 6000 System power supply output is low 12 fozzy.mb.com No
Error 3/20/00 1:56:03 PM HP NetStorage 6000 Primary power cord failure 16 fozzy.mb.com No
Error 3/20/00 1:56:03 PM HP NetStorage 6000 System power supply output is low 12 fozzy.mb.com No
Error 3/20/00 1:55:33 PM HP NetStorage 6000 System power supply output is low 12 fozzy.mb.com No

Chapter 11

Integrating with Remote Backup Applications

Remote Backup Applications Overview

The HP NetStorage 6000 integrates easily with the following remote backup applications:

- ARCserve*IT* (Computer Associates International, Inc.) version 6.61 for Windows NT and UNIX (HPUX and Sun Solaris)
- Backup Exec (VERITAS Software Corporation) Advanced Edition version 7.5 and 8.0 for Windows NT
- HP OpenView OmniBack II version 3.5 for Windows NT and mixed environments (HPUX)

Note These remote backup applications have been extensively tested to be compatible with the HP NetStorage 6000. Additionally, any backup package that can back up a CIFS or NFS mount without using backup agents should be compatible. Contact the software vendors for compatibility information with network attached storage devices.

The information covered in this section pertains only to specific tasks you must perform to use these applications with your HP NetStorage 6000. For further information, refer to the user's manual that came with your backup software.

Using ARCserveIT

ARCserve*IT* is a backup and restore management solution developed to function across various platforms (ARCserve*IT* is a product of Computer Associates International, Inc.). Check the manual that came with your software to see what platforms your edition of ARCserve*IT* supports.

You can use ARCserve*IT* version 6.61 on either a Windows NT or UNIX system connected to your HP NetStorage 6000.

Note	When you back up with a remote server, you cannot use a tape device local to the HP NetStorage 6000.

Using ARCserveIT for UNIX

Before you can backup with ARCserveIT, you must:

- mount on your local host machine the HP NetStorage 6000 volumes you want to back up.
- configure the HP NetStorage 6000 so that the UNIX backup system is set to a trusted host on the HP NetStorage 6000.

To back up files from the HP NetStorage 6000 using ARCserveIT for UNIX:

1. Open a web browser and enter the host name of your ARCserve*IT* backup system in the address field.
2. Click **Backup**.
3. Enter the ARCserve*IT* domain user name and password and click **OK**.
4. In the dialog box, select the default host, then click **OK**.
5. Click **UNIX Agents**, then select the ARCserve*IT* backup host where your HP NetStorage 6000 volumes are mounted.
6. Select the **Node Option** tab, then click **Misc**. Check **Traverse NFS (UNIX Only)**.
7. Click your backup host to expand it.
8. Enter the user name and password of the backup host.
9. Select the HP NetStorage 6000 mount points you want to back up.
10. Select your backup options as you normally would, then start the backup.

Using ARCserveIT for Windows NT

To back up files from the HP NetStorage 6000 using ARCserveIT for Windows NT:

1. Open ARCserve*IT* for Windows NT.
2. Select **Manager** > **Backup**.
3. Select **Network** > **Microsoft Windows Network** > ***Domain Name*** > ***NetStorage 6000 Device***.
4. Select the HP NetStorage 6000 mount points you want to back up.
5. Select your backup options as you normally would, then start the backup.

For more information about using ARCserve*IT*, see the manual that came with the software.

Using Backup Exec

Backup Exec is a high-performance data management solution for Windows NT networks (Backup Exec is a product of VERITAS Software Corporation). The product provides fast, reliable backup and restore capabilities for servers and workstations across the network.

Backup Exec is available in configurations that can accommodate multiplatform networks of all sizes. Check your software to see which edition you are running.

Note When you back up with a remote server, you cannot use a tape device local to the HP NetStorage 6000.

To back up files from the HP NetStorage 6000 using Backup Exec Advanced Edition version 7.3 on a Windows NT server:

1. Open Backup Exec.
2. Select **Tools > Options**. The **Options** dialog box appears.
3. Click the **Network** tab, then check **User Shares**.
4. Select **Entire Network > Microsoft Windows Network >** ***Domain Name > NetStorage 6000***.
5. Select the files or volumes you want to back up.
6. Select your backup options as you normally would, then start the backup.

For more information about using Backup Exec, see the manual that came with the software.

Using HP OpenView OmniBack II

HP OpenView OmniBack II is a backup solution that provides reliable data protection and high accessibility for your data. OmniBack II offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments.

You can use OmniBack II version 3.1 on either a Windows NT or UNIX system connected to your HP NetStorage 6000.

Note	When you back up with a remote server, you cannot use a tape device local to the HP NetStorage 6000.

OmniBack II for UNIX

Before you can backup with OmniBack II, you must:

- mount on your local host machine the HP NetStorage 6000 volumes you want to back up.
- configure the HP NetStorage 6000 so that the UNIX backup system is set to a trusted host on the HP NetStorage 6000.

To back up files from the HP NetStorage 6000 using OmniBack II for UNIX:

1. Open a HP terminal window and type `xomni`, then press **Return** to start OmniBack II.
2. Click the **Backup** icon.
3. Select **Actions > Interactive Backup**. A job editor appears.
4. Select **Object > Add > File System** to add an object to back up. You must choose **File System** to access the HP NetStorage 6000.
5. In the **Backup File System** window, select **Hostname** (the local backup host).
6. Enter a **Mountpoint** (the mountpoint for the NAS volume).
7. Enter a description.
8. Select **Browse**, then highlight the device to back up.
9. Click **Backup Device**, select a device, then click **OK**.
10. Select the files or volumes you want to back up.
11. Select your backup options as you normally would, then start the backup.

OmniBack II for Windows NT

Before you use OmniBack II to back up data from the HP NetStorage 6000, you must enable OmniBack II for Windows NT to back up remote systems.

To enable OmniBack II for Windows NT:

1. Select **Start > Settings > Control Panel**. Double-click **Services**.
2. Locate the OmniBack II Inet Service, then click **Stop**.
3. Click **Startup**, then click **This Account**. Select a valid network administrator account. Create a password, confirm it, then click **OK**.
4. Click **Start** to restart the OmniBack II Inet service.

To back up files from the HP NetStorage 6000 using OmniBack II for Windows NT:

1. Select **Start > HP OmniBack II > OmniBack II Manager**.
2. Verify that **Backup** is selected in the drop-down list in the top left corner of the window.
3. Click the **Tasks** tab on the bottom of the screen, then click **Interactive Backup Wizard**.
4. Change **File System Backup** to **Network Share Backup** in the drop-down list.
5. Click **Map Network Share**.
6. Select **Microsoft Windows Network > *Domain Name* > *NetStorage 6000 Device***.
7. Select the files or volumes you want to back up.
8. Select your backup options as you normally would, then start the backup.

For more information about using OmniBack II, see the manual that came with the software.

Appendix A
Legal Information

Statements

Notice for USA: FCC Class A Product Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference; in such cases, users will be required to correct the interference at their own expense.

Notice for Canada

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Acknowledgments

Outline Java Applet licensed from Byte-Sized Computing (http://www.Byte-Sized.com).

Software License Agreement

IMPORTANT - READ CAREFULLY BEFORE OPENING THIS PACKAGE: OPENING THIS PACKAGE INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS AND IS A REPRESENTATION BY YOU THAT YOU HAVE THE AUTHORITY TO ACCEPT THEM. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU SHOULD PROMPTLY RETURN THE UNOPENED PACKAGE AND YOUR MONEY WILL BE REFUNDED.

This End-User License Agreement ("Agreement") is a binding legal agreement between you (either an individual or a legal entity) and Hewlett-Packard. By opening this Hewlett-Packard software (the "Software") package, you agree to be bound by the terms of this Agreement. (The term Software includes the computer software, the associated media, any printed materials, and any "on-line" or electronic documentation.) If you do not agree to the terms of this Agreement, Hewlett-Packard is unwilling to license the Software to you. In such event, you may not install, use or copy the Software, and you should promptly contact your retailer for instructions on return of the unused product(s) for a refund.

The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software is licensed to you, not sold. Hewlett-Packard retains all right and title to the Software and related documentation.

1 **GRANT OF LICENSE:** This Agreement grants you the following rights:

   a **Software:** You may install and use one copy of the Software on one server computer.

   b **Back-Up Copy:** You may make back-up copies of the Software. You may use the back-up copies solely for archival purposes. You must clearly label any such copies with Hewlett-Packard's copyright notice and any other proprietary legends which appear on the original copy. All copies must be kept in your possession and are the property of Hewlett-Packard.

2 DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

   a **Limitations on Copying and Distribution:** Except as provided in section 1 above, you may not copy, transmit, or distribute the Software, except and only to the extent that such activity is expressly permitted by applicable law despite this limitation.

b **Limitations on Reverse Engineering and Modification:** You may not reverse compile, reverse engineer, decompile, disassemble, convert to a humanly comprehensible form, modify or create works derivative of the Software. You may not disguise, obfuscate the Software in order to use it elsewhere. If the Software is serialized, you may not modify or disable the serial number features nor copy protection mechanisms contained in the Software.

c **Separation of Components:** This Software is licensed as a single product. Its components may not be separated for use on more than one computer.

d **Sublicense, Rental and Third Party Use:** You may not sublicense, rent, timeshare, loan or lease the Software, or directly or indirectly permit a third party to use or copy the Software.

e **Software Transfer:** You may permanently transfer your rights under this Agreement, provided you (i) retain no copies; (ii) transfer all of the Software (including all components, the media, all printed materials, any upgrades, and this Agreement); and (iii) provide Hewlett-Packard with written notice of the transfer within ten (10) days. Any other assignment by you of this agreement shall be void. If the Software is an upgrade, any transfer must include all prior versions of the Software.

f **Export:** You may not export the Software without prior written approval from Hewlett-Packard. If the Software was purchased in the United States of America, you agree to comply with all applicable United States laws and regulations pertaining to export controls. If the Software was purchased outside the U.S., you may not re-export the Software except as permitted by the laws of the United States and the laws of the jurisdiction in which you purchased the software.

g **Termination:** Without prejudice to any other rights, Hewlett-Packard may terminate this Agreement if you fail to comply with the terms and conditions set forth in this Agreement. In such event, you must return all copies of the Software and all of its components and documentation to Hewlett-Packard or certify that you have destroyed all such copies.

3 **COPYRIGHT:** All title and copyrights in and to the Software (including, but not limited to, any images, photographs, animations, video, audio, music, text, incorporated in the Software, the accompanying printed materials, and any copies of the Software) are owned by Hewlett-Packard or its suppliers. You may not copy the printed materials accompanying the Software.

4 **U.S. GOVERNMENT RESTRICTED RIGHTS:** The Software and documentation have been developed entirely at private expense and are provided as "Commercial Computer Software" or "restricted computer software". Use, duplication or disclosure by the U.S. Government or a U.S. Government subcontractor is subject to the restrictions set forth in subparagraph (c) (I) (ii) of the Rights in Technical Data and Computer Software clauses in DFARS 252.227-7013 or as set forth in subparagraph (c) (1) and (2) of the Commercial Computer Software - Restricted Rights clauses at FAR 52.227-19, as applicable. The Contractor is Hewlett-Packard Company, 3000 Hanover Street, Palo Alto, California 94304.

5 **LIMITED WARRANTY:** Hewlett-Packard warrants that the Software will perform substantially in accordance with the applicable Hewlett-Packard published documentation prevailing at the time of shipment for a period of ninety (90) days from the date of receipt. Hewlett-Packard warrants that any media accompanying the Software will be free from defects in materials and workmanship under normal use and service for a period of ninety (90) days from the date of receipt. Any implied warranties on the Software and media are limited to ninety (90) days. Some states or jurisdictions do not allow limitations on the duration of an implied warranty, so the above limitation may not apply to you.

6 **CUSTOMER REMEDIES:** Hewlett-Packard's entire liability and your exclusive remedy shall be, at Hewlett-Packard's option, either (a) return of the price paid, or (b) repair or replacement of the Software that does not meet the limited warranty in section 5 above and which is returned to Hewlett-Packard with a copy of your receipt. Any replacement Software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

7 **NO OTHER WARRANTIES:** YOU ACKNOWLEDGE AND AGREE THAT THE USE OF THE SOFTWARE IS AT YOUR OWN RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HEWLETT-PACKARD AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. HEWLETT-PACKARD DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE AND RELATED

DOCUMENTATION WILL BE CORRECTED, FURTHERMORE, HEWLETT-PACKARD DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE RESULTS OF THE USE OF THE SOFTWARE OR RELATED DOCUMENTATION IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY HEWLETT-PACKARD OR A HEWLETT-PACKARD AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE HEWLETT-PACKARD SOFTWARE PROVE DEFECTIVE, YOU (AND NOT HEWLETT-PACKARD OR A HEWLETT-PACKARD AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS WHICH VARY FROM STATE OR JURISDICTION TO STATE OR JURISDICTION.

8 **NO LIABILITY FOR CONSEQUENTIAL DAMAGES:** TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL HEWLETT-PACKARD OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR INDIRECT DAMAGES FOR PERSONAL INJURY, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF HEWLETT-PACKARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, HEWLETT-PACKARD'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS AGREEMENT SHALL BE LIMITED TO THE PRICE PAID FOR THE SOFTWARE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

9 **INDEMNITY:** You agree to indemnify and hold Hewlett-Packard and its suppliers harmless from and against any and all claims of any kind (along with attorney's fees and litigation costs), including but not limited to, personal injury or property damage arising out of, resulting from, or in connection with results you have obtained through your negligent use or misuse of the Software.

10 GOVERNING LAW: This Agreement is governed by and construed in accordance with the laws of the State of California, U.S.A as applied to agreements entered into and wholly performed within California between California residents. This Agreement shall not be governed by the 1980 U.N. Convention on Contracts for the International Sale of Goods.

11 COMPLETE AGREEMENT: This Agreement is the entire agreement between Hewlett-Packard and you with respect to the Software. THE ACCEPTANCE OF ANY PURCHASE ORDER PLACED BY YOU IS MADE CONDITIONAL ON YOUR AGREEMENT TO THE TERMS SET FORTH IN THIS AGREEMENT, AND HEWLETT-PACKARD AGREES TO FURNISH THE SOFTWARE ONLY UPON THESE TERMS AND NOT UPON THOSE IN YOUR PURCHASE ORDER. This Agreement replaces all prior understandings and agreements, whether written or oral. This agreement may not be modified unless Hewlett-Packard and you both assent in writing.

12 SEVERABILITY: If for any reason a court of competent jurisdiction finds any provision or part of any provision of this Agreement unenforceable, that part or provision shall be enforced to the maximum extent permitted by law so as to effect the intent of the parties, and the remainder of the agreement shall continue in full force and effect.

Appendix B

NetStorage 6000 Warranty Information

Planning for Support

1. Retain your Proof-of-Purchase

   Affix your original proof-of-purchase (sales receipt) to the inside cover of this User's Guide. Support of your system is based on length of ownership. You may need this information should you have to contact HP for post sales support. If you do not have a copy of your proof-of-purchase, please contact your internal purchasing department.

2. Record Product and Serial Numbers

   Please record the product number and product serial number in the space provided below. The product and serial numbers are located inside the front panel of your HP NetStorage 6000. This will help us help you quicker.

   Product Number:

   _____

   Product Serial Number:

   _____

3. Register Your Product

   If you did not register your product during the Setup & Installation process, it's not too late! To register your product, simply go to the HP Customer Care web site at http://www.hp.com/support/NS6000 and follow the on-line instructions. Registering your product is easy, only takes a few minutes, and brings you many benefits, including:

   - The ability to customize your Proactive Notification Profile, specifying the kind of product or Service & Support updates you want HP to automatically send you in relation to this product.
   - Receive personalized and more expedient technical web & telephone support customized to your product and its operating environment.
   - Access to driver & OS upgrades.
   - Opportunity to participate in on-line Forums.
   - Access to white papers & technical documents.

- Access to Troubleshooting Trees that help you diagnose and resolve your own support issues.
- Opportunity to service your own products through participation in HP's Self-Maintenance Program.
- E-mail access to HP Support Engineers

4 Become a Self-Maintainer (optional)

Once you have registered your product, you automatically qualify to participate in the HP Self-Maintenance Program. This program has been designed to provide customers the opportunity to service their own products without having to rely on a HP Service Engineer to arrive on-site. The HP Self-Maintenance Program, coupled with the Customer Replaceable Parts program, puts you in control of your service experience, allowing you to perform the same repair services that would normally be provided by a HP Service Engineer.

To find out more about the HP Self-Maintenance Program and take advantage of this offer, contact the HP Self-Maintenance Support Line at 1-208-227-8164 (7am-6pm PT).

5 Warranty Upgrades (optional)

HP offers a variety of SupportPack products that provide you the opportunity to upgrade your standard warranty. Please contact your HP Authorized Reseller or the HP Customer Support Business Center at 1-800-743-8305 for information on upgrading your warranty.

Obtaining Warranty Support

1 Diagnose the Problem

If you encounter difficulty with your HP NetStorage product, refer to the Monitoring and Troubleshooting chapter of this User's Guide to troubleshoot or identify the failing component in your product.

If you are unable to resolve your issue, log onto the HP Customer Care Web Site at http://www.hp.com/support/NS6000 for additional troubleshooting assistance. This site is frequently updated with the latest troubleshooting tools, technical specifications, and driver and OS upgrades - specific to your HP NetStorage product.

Note Access to some content may be limited to registered customers only. Refer to Step 3 of Planning for Support for information on registering your product.

2 Initiate a Service Request

If you are unable to resolve your problem using the tools provided by HP, you may contact the HP Authorized Reseller who sold you your HP NetStorage product or you may contact HP directly. If you are not sure if your Reseller is authorized by HP to service your HP NetStorage product, use the HP Service Locator to find a HP Authorized Support Provider in your area. HP's Service Locator can be accessed at http://www.hp.com/service_locator.

Should you choose to contact HP directly, please call the HP Customer Care Center in your region, during the hours specified below, where a HP Service Engineer will assist you with troubleshooting, placing part orders or processing any on-site service requests that may result out of your support experience.

Region	Telephone Number	Hours of Operation
Canada	905-206-4663	M-F, 6am-6pm MT
United States	970-635-1000	M-F, 6am-6pm MT

Prior to contacting a HP Customer Care Center, please be prepared to provide the following information:

- HP product number
- Product serial number
- Date of purchase
- Your name and shipping address
- Operating environment details (such as, operating system, manageability tool)
- Description of problem (such as, application error message from system or diagnostics)
- Third party hardware or software
- Operating system type and revision
- Troubleshooting performed

HP Self-Maintainer processes may vary; please refer to the on-line program participation instructions available on the HP Customer Care web site at http://www.hp.com/support/NS6000.

If you have upgraded your warranty with a HP SupportPack, please follow the instructions for obtaining support outlined in your HP SupportPack Agreement.

Obtaining Out-of-Warranty Support

1 Diagnose the Problem

If you encounter difficulty with your HP NetStorage product, refer to Monitoring and Troubleshooting chapter of this User's Guide to troubleshoot or identify the failing component in your product.

If you are unable to resolve your issue, log onto the HP Customer Care Web Site at http://www.hp.com/support/NS6000 for additional troubleshooting assistance. This site is frequently updated with the latest troubleshooting tools, technical specifications, driver and OS upgrades - specific to your HP NetStorage product.

Note Access to some content may be limited to registered customers only. Refer to Step 3 of Planning for Support for information on registering your product.

2 Placing Part Orders

To order service parts after your warranty has expired, please contact the appropriate HP Customer Care Parts Ordering center in your region, during the hours specified below.

Region	Telephone Number	Hours of Operation
Canada	800-387-3154 or 905-206-4747	M-F, 8:30am-5pm ET
United States	800-227-8164	M-F, 6am-5pm PT

Note Self-Maintainer processes may vary. Please refer to the program and participation information located on the HP Customer Care web site at http://www.hp.com/support/NS6000.

Hewlett-Packard Limited Warranty Statement

1 HP warrants to you, the end-user customer, that HP hardware will be free from defects in materials and workmanship for a period of ONE (1) YEAR from date of purchase. If HP receives notice of such defects during the warranty period, HP will, at its option, either repair or replace product components that prove to be defective. Replacement components may be either new or equivalent in performance to new.

a Repair or replacement will be performed by HP, Reseller or qualified third party, at HP's option, "on-site" at your premises or by use of the Customer Replaceable Part process The following table outlines HP's response time goals based on distance. Response times are not guaranteed.

Zone	Distance from HP Office	Response Time
1-3	160 km (100 mi)	Next Business Day
4-5	320 km (200 mi)	Second Business Day
6	480 km (300 mi)	To be negotiated
Not designated	Over 480 km (300 mi)	To be negotiated

b On-site service is restricted or unavailable in certain locations. In HP-Excluded Travel Areas-areas where geographical obstacles, undeveloped roads, or unsuitable public transportation prohibit routine travel-service is provided on a negotiated basis at extra charge. To find out if you are in a geographically restricted service area, contact the HP Customer Support Business Center at 1-800-743-8305

c HP SupportPacks and other enhanced services may follow different guidelines. Please contact your HP Authorized Reseller or the HP Customer Support Business Center at 1-800-743-8305 for information warranty upgrades and response times.

2 Replacement components assume either the remaining warranty of the components they replace or 90 days, whichever is greater. When service involves the exchange of a product or a component, all removed components, in their entirety, become the property of HP and must be returned to HP after the replacement has been installed. The replacement component becomes your property and you may be billed for components not returned to HP.

Caution Use only HP Hard Drives approved for your NetStorage 6000. For an up-to-date list of approved hard disk drives, please visit our web site at http://www.hp.com/support/ns6000. Drives on the approved list have custom firmware for use in your NetStorage 6000. Do not attempt to install any hard disk drives other than the approved drives listed at this web site as doing so may result in system failure or loss of data. Using non-supported hard drives may also void your warranty.

3 This Limited Warranty does not apply to defects resulting from (a) improper or inadequate maintenance or calibration, (b) software, interfacing, parts, or supplies not supplied by HP, (c) unauthorized modification or misuse, (d) operation outside of the published environmental specifications for the product, (e) acts of God, or (f) improper site preparation or maintenance.

4 HP does not warrant that the operation of HP products will be uninterrupted or error free. If HP is unable, within a reasonable time, to repair or replace a product, confirmed by HP to be defective due to reasons other than those described in #2 above, to a condition as warranted, you will be entitled to a refund of the purchase price upon prompt return of the product.

5 TO THE EXTENT ALLOWED BY LOCAL LAW, THE ABOVE WARRANTIES ARE EXCLUSIVE AND NO OTHER WARRANTY OR CONDITION, WHETHER WRITTEN OR ORAL, IS EXPRESSED OR IMPLIED AND HP SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR CONDITIONS, OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE. Some countries, states, or provinces do not allow limitations on the duration of an implied warranty so the above limitation or exclusion might not apply to you. This Limited Warranty gives you specific legal rights and you might also have the rights that vary form country to country, state to state, or province to province.

6 HP will be liable for damage to tangible property per incident up to the greater of $300,000 or the actual amount paid for the product that is the subject of the claim.

7 TO THE EXTENT ALLOWED BY LOCAL LAW, THE REMEDIES IN THIS LIMITED WARRANTY STATEMENT ARE YOUR SOLE AND EXCLUSIVE REMEDIES. EXCEPT AS INDICATED ABOVE, IN NO EVENT WILL HP BE LIABLE FOR LOSS OF DATA OR FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL (INCLUDING LOST PROFIT OR DATA), OR OTHER DAMAGE,

WHETHER BASED IN CONTRACT, TORT OR OTHERWISE. Some countries, states, or provinces do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

8 THE WARRANTY TERMS CONTAINED IN THIS STATEMENT, EXCEPT TO THE EXTENT LAWFULLY PERMITTED, DO NOT EXCLUDE, RESTRICT, OR MODIFY, AND ARE IN ADDITION TO THE MANDATORY STATUTORY RIGHTS APPLICABLE IN YOUR JURISDICTION TO THE SALE OF THIS PRODUCT TO YOU.

Appendix C
System Specifications

Central Processing Unit (CPU)

Physical Characteristics

Height	22.2 cm (8.75 in)
Width	48.3 cm (19.0 in)
Length	66.0 cm (26.0 in)
Rack Height	5 U
Weight	42 kg (93 lbs) [typical with 10 HDDs]

Power Requirements

Voltage Range	100V/120V/220V/240V ±10% VAC
Frequency	50-60 ±5% Hz
Power Consumption	450 watts (with 10HDDs)

Uninterruptible Power Supply (UPS)

Note Not HP Supplied. Provided for user reference only. Please consult APC documentation for updated specifications.

Supported UPS: APC Smart-UPS 2200

Physical Characteristics

Height	8.9 cm (3.5 in)
Width	48.3 cm (19.0 in)
Length	45.7 cm (18.0 in)
Rack Height	2 U
Weight	21.8 kg (48.0 lbs)

Power Requirements

Input Voltage Range	0 - 160 VAC
Output Voltage Range	115 nominal VAC
Frequency	50 or 60 Hz ±5% (auto sensing)
Power Consumption	Not specified

Performance

- EMI/RFI filtering
- No power cold starts
- Intelligent battery management
- Six power output receptacles
- One output and one input circuit breaker
- User-replaceable batteries
- Automatic 14-day self-test
- User-selectable low battery warning level
- User-selectable voltage sensitivity

Hardware Specifications

In this section you can find information on the following specifications for the HP NetStorage 6000:

- Performance Specifications
- Features
- Upgrade Options
- Security and Safety
- Regulatory Compliance
- Environmental Specifications
- Power Specifications

Performance Specifications

Hardware	Specification
Processor	Intel Pentium III 700MHz, Slot 1 with 256KByte on CPU Cache; ECC Protected
Memory	• 256MB SDRAM (2x128MB DIMMs) • ECC capable with hardware error scrubbing; Corrects single bit errors, detects multiple bit errors • Unbuffered and registered DIMMs may not be mixed
I/O Expansion Slots	• Three PCI slots • One ISA slot • One shared ISA/PCI slot
Video, Keyboard, Mouse, CD-ROM, Flexible Disk Drive	Not supported
Built in I/O Ports	• Serial Communications port for UPS monitoring (DB9 male) • Serial Communications port for TTY interface for system debug and status when system cannot boot to network
Embedded OS	• 32MB FLASH ROM for fast, reliable OS loading • Support User upgrade of system OS FLASH contents

Hardware	Specification
User Interface	• 2x20 LCD with back light for initial system configuration and status/ error monitoring • Four pushbutton switch interface • Front panel controls for on front panel for: • Network configuration: IP address, gateway IP, and subnet mask • System operation: initiating system shutdown or reboot, silencing audible alarms • Single push-button switch interface on front panel for silencing audible alarm
Disk Drive Interface	Wide Ultra2 SCSI, SCA connector
Minimum Raw Storage Capacity (RAID 5)	72GB (3x36GB drives, RAID5, additional hot spare can be added)
Maximum Raw Storage Capacity (RAID 5)	Up to 10 Ultra2 SCSI disks • 288GB (10x36GB drives)[a]
Maximum RAID5 Group Size	Up to 8 drives per RAID5 group
Available Network Interfaces	• Supported by add in PCI card • Vendors/Cards supported • 10/100TX • Half or full duplex • RJ-45 connector • Dual 10/100TX • Half or full duplex • RJ-45 connector • Gigabit Ethernet • Half or full duplex • 1000BASE-SX (fiber)
External Tape Backup Device Support	• Supported by included PCI card • Wide SCSI 68 pin connector

a. Disks configured as two RAID5 groups of 5 drives each, no hot spare available.

Features

Feature	Description
Self-restart Capability	Automatic Server Restart (ASR) that reboots incase of embedded NOS hang
Environmental Monitoring	Temperature, voltage, and fan-speed monitoring with alarm capability
Self-Correcting Memory	ECC capable with hardware error scrubbing; corrects single bit errors, detects multiple bit errors
Hot-Swap Subsystem	• Supports 36GB and future low profile and half height SCSI hard disks • Up to 10 hard disks
RAID Disk Array Controller	• Hardware RAID accelerator with 32MB of NVRAM • RAID5 • Supports up to 10 hard disks with hot swap • Maximum RAID5 group of 8 drives • 32MB NVRAM for cached write protection • Support for SMART capable disk drives • Automatic detection of hard disk failure with automatic rebuild to global hot spare
Power Supply Modules	• Triple, redundant with hot swap • System can tolerate failure of one supply (two required for minimum operation) (2+1 operation) • Audible alarm and network alarm for failure
Fans	• 2 Redundant fan assemblies with fan-speed monitoring for system cooling • Fan hot swap supported
Boot Time	Seconds from power on to file system available (after proper shutdown, one 5 drive RAID5 partition, typical)
UPS Support	• External Uninterruptible Power Supply (UPS) monitoring through integrated serial port (DB9 male) • System shutdown initiated battery critical error reported by UPS • Requires Sine-wave output • Support for the following APC Brand UPS: • APC Smart-UPS 700 Model APC SU700RMNET

Upgrade Options

Upgrade	Description
Disk Storage Capacity	Up to 10 SCSI disk drives, hot swap capable, industry standard 3.5" low profile or half height form factor
Extra Drive Bays	None available (backup solution must be in external package)
System Memory	• 256MB SDRAM (2x128MB DIMMs) • ECC capable with hardware error scrubbing; corrects single bit errors, detects multiple bit errors
Additional Network Interfaces	• Supported by add in PCI card • Vendors/Cards supported • 10/100TX • Half or full duplex • RJ-45 connector • Dual 10/100TX • Half or full duplex • RJ-45 connector • Gigabit Ethernet • Half or full duplex • 1000BASE-SX (fiber)

Security and Safety

- Chassis lock behind front door to secure disk drive shuttles
- Key compatible with HP part number 5063-5683

Regulatory Compliance

Category	Country or Region	Specifications
Electromagnetic Emissions Design Goal: 4 dB margin to specified emissions limits	USA	• FCC Class A Verified • 47CFR parts 2 and 15 • 10 meter test distance for radiated emissions • ANSI C63.4-1992 test procedure • CISPR 22:1993 Class A at 10 meters test limits • FCC Class A Conducted Emissions • Test at A2LA or NVLAP accredited test facility
	Canada	• Industry Canada (Accepts FCC test results) • Interference Causing Equipment Standard ICES-003 Issue 3 1997 • Canadian Standards Association CAN/CSA-CISPR 22-96 test methods and limits • Class A
Safety Compliance	-	• CSA Certified (Canada) or cUL Listed • UL Listed (USA)

Environmental Specifications

The HP NetStorage 6000 is a Hewlett-Packard environmental class C1 product. All specs herein, unless otherwise noted, are per the HP Corporate Quality Environmental Tests. Class C1 is defined as follows:

Section 751.005

4.5 Class C1 - Controlled Office Environment. This classification applies to office and computer equipment intended for use under moderate temperature and humidity limits only. Other environmental factors are similar to Class B2 (General Purpose Environment). Special attention to Acoustical noise and ergonomic issues must be provided. This class should not be used for personal computers, terminals, or system peripherals that will have a market application in systems associated with Class B2.

Specification	Description
Operating Temperature	+5 to +35° C (+45 to +95° F)
Storage Temperature (non-operating)	-40 to +70° C (-40 to +140° F)
Operating Humidity	20% to 80%, non-condensing
Storage Humidity (non-operating)	10% to 90%, non-condensing
Operating Altitude	0 to 3,048 m (0 to 10,000 ft)
Storage altitude (non-operating)	4,572 m (15,000 ft)
ESD	• Air Discharge - Continued Functionality: 0 to 10kV • Air Discharge - Hardware Survival: 0 to 25kV • Contact Discharge - Continued Functionality - 0 to 4kV • Contact Discharge - Hardware Survival - 0 to 4kV
Vibration - Operating & Functional	Random (5 - 500Hz) 0.0001g^a/Hz

Specification	Description
Vibration - Survival	• Swept Sine (5-500 Hz, 0.5g (0 to Peak), sweep rate 1 oct/min, 5 minute dwell at 4 resonances - per axis while product is powered up) • Random (5-500 Hz, ~2.41 G_{rms}, 5-100 Hz @ 0.015 g*/Hz, 100-137 Hz @ -6 dB/oct slope, 137-350 Hz @ 0.0107 g* /Hz, 6 dB/oct slope, 500 Hz @ 0.0052 g*/Hz, 10 minutes each axis (min.) while product is powered up)
Shock (End Use Handling)	Less than 45.5 kg: Shock Machine Test, Half sine waveform, <3 millisec duration, velocity change equals: delta Velocity = 171-0.69m for 9.1<m<45.4kg
Shock (Transportation)	Shock machine test with trapezoidal waveform and velocity change per table below:
	Type 1: Single or multiple products, boxed, non-paletized, which may be shipped as a single unit to the end user.
	Type 2: Single product, palletized and prepared for shipment such that it's orientation is intended to be controlled.
	Type 3: Multiple products, unitized and palletized, which are shipped only as a palletized load to the end user.
Package Test (Vibration)	And
Package Test (Impact)	
Acoustics	5.0 Bels (sound power as calculated from the sound pressure measurements power ISO Standards requirements)
System Dimensions	Desktop: 8 ¾" H x 19" W x 22" D Rack: 5U (8 ¾") H x 19" W x 22" D
System Weight	38-42 kg (85 - 93 lbs)

Specification	Description
MTBF (Mean Time Between any Failure)	53,500 hours at 25oC, 10 Disk Drives
MTBCF (Mean Time Between Critical Failure)	490,000 hours
MTTDL (Mean Time to Data Loss)	Greater Than 1,000,000 hours (RAID5 required)
Mean Life Requirement	35 Years
Availability	Better than 99.99%

a. Tests made while operating on the 120V range.

Power Specifications

Specification	Description
Power Line	• 100V/120V/220V/240V ±10% • 50Hz and 60Hz ±5%
Power Line Transient	• Low Energy Pulse - 3KV / 100kHz Ring Wave • High Energy Pulse - 1KV at 1.2 Microsec by 50 Microsec
Recoverable Power Line Surge	From 129V to 150V for 500 millisec[a]
Recoverable Power Line Sag	From 108V to 80.5V for 500 millisec
Power Line Dropout	From lower limit to 0V for 10millisec - Transparent to user
Power Availability	500 W maximum
Power Consumption	450 W typical, 10 HDDs installed

a. Tests made while operating on the 120V range.

Replacements and Upgrades

Hewlett-Packard offers hardware replacements for the HP NetStorage 6000.

Note These replacements should be on hand prior to failure so the new part can be installed quickly.

HP offers these kits:

- Fan replacement kit
- Hard drive replacement kit
- Power supply replacement kit
- SureCare kit (includes each of the above kits)
- Hewlett-Packard also offers several hardware upgrades for the HP NetStorage 6000. They are:
- Storage upgrade, which allows you to add three (a new RAID set) or more drives to your current system.
- Network interface card upgrade, which allows you to add different networks to your system.
- Desktop conversion, which lets you make the unit more presentable for desktop usage instead of rack mounting.

You can not replace the SCSI Host Adapter.

For replacements and upgrades, use only HP hardware. To order one or more of the kits, call 1-800-227-8164.

Appendix D
Telnet Information

Telnet is a text-based interface (analogous to the web interface). The Telnet interface is hosted/served by the server and does not require you to install any software on your system (if you have a Telnet applet).

To access Telnet:

1. Run your Telnet applet and specify the host name or IP address of the server.
2. Once you are connected, the interface prompts you to enter a command. Press **Enter** or type `Menu`. A menu-driven interface appears.
3. Review the screen and enter commands as necessary to complete your task.

For more information on Telnet, see *Managing the HP NetStorage 6000 Using Telnet*. You can view this guide on the web at http://www.hp.com/support/ns6000/.

Appendix E
Troubleshooting and Error Codes

General Issues

Problem	Solution
The storage device does not power on.	• Make sure the cables are connected correctly and securely. The primary power cord needs to be connected when power is turned on. • Cycle the power switch on and back on. This is always required after a soft or remote shutdown.
The Windows environment does not recognize the HP NetStorage 6000 machine name.	If you use machine names to define parameters in the **Configuration** tab, you must map your IP address to a machine name. Make sure: • the addresses of the WINS servers are entered in the **Configuration** tab under **Network Settings > Windows Settings**. • the Domain Name Server is entered in the **Configuration** tab under **Network Settings > TCP/IP Settings**. • these servers are running. • the system name on the HP NetStorage 6000 matches the entry on the DNS server.
The Windows environment does not see the HP NetStorage 6000 volumes or directories.	• Make sure the volumes or directories have the been shared appropriately. Click the **Storage** tab, then select **File Volumes** and view the file volume summary. • Make sure there is no IP address conflict with another computer. Click the **Status** tab, then select **Event Log** and look for IP conflict messages.

Problem	Solution
What happens if a drive fails?	If a disk drive is assigned as a hot spare, the system automatically switches to the hot spare and rebuilds the data on the failed drive. During this process, the hot spare becomes a member of the RAID set, and the system continues to serve files without interruption. System warnings alert you that a drive failure has occurred. When the failed drive is replaced, you must manually assign the new drive to be the new hot spare. The drive replacement kit provides detailed instructions.
What happens if a drive fails and there is no hot spare?	HP recommends that at least one drive be assigned as a global hot spare at all times. If a drive fails and no hot spare is present, system warnings alert you that a drive failure occurred and that the logical drive (RAID set) is in a critical state. Although the system continues to rebuild and serve files without interruption, there is a much greater risk of data loss in this state. The drive replacement kit provides detailed instructions for installing replacement drives, rebuilding the critical RAID set, and assigning a hot spare.
How do I turn off the alarm?	Push the alarm reset button on the front panel.
Can I connect a monitor, keyboard, and mouse to the HP NetStorage 6000?	HP does not recommend that you make these connections.
How do I communicate with the system without a network connection?	The HP NetStorage 6000 has a serial TTY connection that can be used to access the system without a network connection. To use it, connect the TTY port to another computer using the supplied serial cable. A terminal emulation program can then be used to interact with the system's menu-driven console interface (this is the same as the Telnet interface).
Why can't I access Tape Status, Tape Backup, Tape Restore, and Tape Settings in the Backup/Restore tab?	These screens are accessible only *after* you attach either an 818 or 1/9 HP SureStore DLT Autoloader to your HP NetStorage 6000.

Problem	Solution
How do I create UNIX mount points?	The HP NetStorage 6000 automatically generates a UNIX mount point at the root of a file volume when you create the volume. Thus, there is no need to manage mount points on a directory by directory basis. Refer to your UNIX users guide for more information about mount points.
My version of the syslog is not automatically displaying HP NetStorage 6000 event log entries in the system log file.	Red Hat Linux 6.1 requires that you set the -r option in the syslog daemon to enable the device to receive messages from the network. This action, along with defining the remote server on the SYSLOG page, allows the HP NetStorage 6000 event log messages to appear in the Red Hat Linux 6.1 system log file.

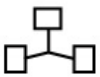
Browser Issues

Problem	Solution
The web browser does not connect to the unit.	Try disabling the proxy on the web browser, or exclude intranet addresses.
The IP address does not respond to the web browser.	• Make sure the unit accepted the IP address entered in the front panel display. Recheck the IP address on the front panel. • Make sure the network connection is working. Ping the unit (open a command prompt, then type `ping` and the unit's IP address) from another networked computer. If the unit does not respond, check network connections and topology. • Make sure there is no IP address conflict with another computer. The easiest way to determine this is to turn off the unit and ping it again. If the unit responds while it is turned off then you have an IP conflict. Alternatively, the Telnet or TTY interface event log displays an IP conflict message when one exists.
The NetStorage web interface pages are not displaying correctly.	The NetStorage web interface uses Java components to properly display system information. These components require secure access to the HP NetStorage 6000. As a result, your browser may generate a security warning. You must accept content from or grant privileges to Hewlett-Packard Company. If you fail to do so, you must restart your browser and accept content from or grant privileges to Hewlett-Packard Company. To prevent further security warnings from appearing, check the box at the bottom of the security warning window.

Problem	Solution
The NetStorage web interface pages are not displaying correctly in Internet Explorer.	Microsoft's Internet Explorer/Java Virtual Machine may not have been installed properly. If this is the case, Java applets will not run properly. See Microsoft Knowledge Base article Q168806. In particular, pay attention to where the registry entry `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Global Namespace\Java Packages\com\ms\lang\Path` refers to. Copying the correct file to the file referred to by the registry fixes the problem. The correct file is generally in the directory referred to by the registry and is about 5 to 6 megabytes in size.
The NetStorage web interface in Netscape is small and unreadable on my HP-UX machine.	**1** Change the browser fonts from HP fonts to Sun fonts to improve the interface appearance. To do this, set the environment variable MOZILLA_JAVA_FONT_PROPERTIES to $MOZILLA_HOME/java/classes/sun. If this doesn't help, try option 2. **2** You need to change your font settings in the browser. Select **Edit > Preferences > Appearance > Fonts** and click **Use my default fonts**. This overrides document-specified fonts. You may also need to increase the font size (select **View > Increase Font**).
The NetStorage web interface pages are not displaying on my HP-UX machine.	The README file for Netscape Navigator on UNIX tells you to set the CLASSPATH environment variable to include the path to the Java jar file. However, the web interface pages will not display correctly. Set the CLASSPATH environment variable to *exclude* the path to the Java jar file.

Determining Component Failure

LED	Light	Cause	Solution
Power Status	Blinking red	Power supply failure	**1** Turn off the alarm by pressing the alarm reset button on the front panel. The power status LED continues to flash as long as the power failure remains. **2** Verify that a power supply has failed by looking at the rear of the unit. The LED on the failed power supply will be blinking red or off. **3** Replace the failed power supply. The power supply replacement kit provides instructions.
	Off	No power to system	• Verify that the master power switch is on. The switch may have to be cycled off and on. • Power modules not present or not latched. Check installation of power modules. • Multiple power supply failure. Call your HP service representative. • Power system failure. Call your HP service representative.
Fan Status	Blinking red	Fan failure	**1** Turn off the alarm by pressing the alarm reset button on the front panel. The fan status LED continues to flash as long as the power failure remains. **2** Verify that a fan has failed by looking at the rear of the unit. The LED on the failed fan will be blinking red or off. **3** Replace the fan. The fan replacement kit provides instructions.
General Alert	Blinking red	Power cord or source failure	Check power cord connections and sources. If necessary, change power sources and connections one-at-a-time so that no power interruption occurs to the unit.

LED	Light	Cause	Solution
		Temperature out of range	• Check ambient temperature (must be below 35° C). • Remove airflow restrictions at the front and back faceplates. • Check fan status reported on front panel and in NetStorage web interface. • Replace any failed system blowers, or call an HP service representative if the CPU fan has failed.
Network Activity 	Blinking red	All network links are bad or unattached	• Check network cable and connections. • Check hub/switch port function and protocol settings.
Drive Active (top row of LEDs on the front panel)	Off	Hard drive not fully seated	Tighten the screw.
	Blinking yellow	Drive initializing or rebuilding	No action required.
	Blinking red	Drive failure	Replace the drive. The drive replacement kit provides detailed instructions.

UPS Troubleshooting

Not HP Supplied. The following UPS troubleshooting information is provided for your convenience. Please contact APC directly if you have questions (model number APC Smart-UPS 2200). See your UPS manual for contact information.

Problem	Possible Cause	Solution
UPS will not turn on.	UPS input circuit breaker tripped.	Reduce the load on the UPS by unplugging equipment and reset the circuit breaker by pressing the plunger back in.
	Very low or no utility voltage.	Check the AC power supply to the UPS with a table lamp and if the lamp is dim, have the voltage checked.
UPS will not turn on or off.	Computer interface or accessory problem.	Disconnect the computer interface or accessory. If the UPS now works normally, check the interface cables, the computer and attached accessories.
UPS operates on battery even though normal line voltage is thought to exist.	UPS input circuit breaker tripped.	Reduce the load on the UPS by unplugging equipment and reset the circuit breaker by pressing the plunger back in.
	Very high, low or distorted line voltage.	Test the input voltage with the utility voltage display. Inexpensive fuel powered generators can distort the voltage. If acceptable to the load, reduce the UPS sensitivity.
UPS beeps occasionally.	Normal UPS operation.	None.
UPS does not provide expected back-up time.	UPS battery is weak due to recent outage or is near the end of its service life.	Charge the battery. The UPS batteries require charging after an extended power outage.
	UPS is overloaded	Check the UPS load display. Unplug the less important equipment, such as a printer.
Front panel indicates flash sequentially.	UPS has been shutdown by remote control.	None.
All indicators are lit and the UPS emits a constant tone.	Internal UPS fault.	Do not attempt to use the UPS. Turn the UPS off and have it serviced immediately.

Problem	Possible Cause	Solution
Low Battery LED is lit and the online LED is off.	UPS is shutdown and the battery is discharged from an extended power outage.	None.
Replacement Battery LED is lit.	Weak batteries.	Allow the batteries to recharge for at least four hours. If the problem persists after recharging, replace the batteries.
	Replacement batteries not properly connected.	Confirm the battery connections.

Hardware Error Codes

When errors occur in the subsystems, the HP NetStorage 6000 generates error messages. The system notifies you of errors in any of the following ways:

- Traps
- Event log
- E-mail
- LCD
- Web interface

Network management applications (HP TopTools, HP OpenView Network Node Manager, Computer Associates Unicenter TNG Framework) display trap messages. The HP NetStorage 6000 displays event log messages. The event log and email notifications give you the time the error occurred. If one or more actions fail, the failed actions repeat in the next monitoring cycle.

Trap Message	Event Log Message	E-mail Message	LCD Message	Web Interface Message	Solution
Partition X is full.	File system *FilesystemName* usage capacity of system at location *sysLocation* is at *fileSysThreshold* %	-	F40 *File System Name* Full	The space used on this volume has exceeded the predefined threshold.	Free up space by migrating files off the Volume.
RAID controller X failed.	-	-	-	The RAID controller is not functioning correctly.	Contact your local Service Representative.

Trap Message	Event Log Message	E-mail Message	LCD Message	Web Interface Message	Solution
The disk in slot X failed.	-	-	-	A physical drive in the RAID set has failed.	We recommend that you promptly replace the failed drive. If a hot spare drive is available, the system will automatically rebuild the RAID set using this spare. If a spare is not available and a second drive in this RAID set fails, all data will be lost.
A RAID set failed due to a disk failure.	NetStorage 6000 RAID set failed due to a disk failure.	Raid Controller N of system at location *sysLocation* failed.	-	A RAID set on the system has failed. This is usually caused by more than one physical disk drive failure.	We recommend replacing the failed drives, reconstructing the storage environment, and restoring data from a tape backup.
A UPS failed.	UPS failure in system at location *sysLocation*.	-	U25 UPS failure	-	Replace the failed UPS.
The battery is low or overloaded.	Low battery condition at system in location *sysLocation*.	Low battery condition at system in location *sysLocation*.	U22 low battery	-	-
Replace the battery.	UPS battery in system at location *sysLocation* needs to be replaced	-	U23 UPS battery replace	-	-
The power supply X output is low.	Power supply xx in the system at location yy is in critical condition: the output is under range.	Power supply xx in the system at location yy is in critical condition: the output is under range.	-	Power module x - power warning. Status>Summary	Replace power supply as soon as possible. The power supply replacement kit provides instructions.

Trap Message	Event Log Message	E-mail Message	LCD Message	Web Interface Message	Solution
The power supply X temperature is too high.	Power supply xx in the system at location yy is in critical condition: the temperature is in a critical range.	Power supply xx in the system at location yy is in critical condition: the temperature is in a critical range.	P22 Power (X) overheat	Power module x - temperature warning.	Verify that the power supply switch and master power switch are both turned on. Replace power supply. The power supply replacement kit provides instructions.
The power supply X has no AC power.	Power supply xx in the system at location yy is in critical condition: the AC power is not detected.	Power supply xx in the system at location yy is in critical condition: the AC power is not detected.	-	Power module x - AC warning.	Check to insure that the power supply is properly secured in the unit. Replace the power supply if this is not effective.
NetStorage 6000 fan x failed.	Fan xx in the system at location yy failed.	-	-	-	Replace fan.
The primary power cord failed.	The primary power cord in the system at location yy failed.	The primary power cord in the system at location yy failed.	P31 Primary power cord failed	-	Re-establish good connection with power cord or replace power cord.
The secondary power cord failed.	The secondary power cord in the system at location yy failed.	The secondary power cord in the system at location yy failed.	P32 Secondary power cord failed	-	Re-establish good connection with power cord or replace power cord.

Trap Message	Event Log Message	E-mail Message	LCD Message	Web Interface Message	Solution
-	Operator reset the system at location yy.	-	P41 Operator reset.	-	No action required.
-	Disk drives failure in system at location *sysLocation*. Failed drives are: *Drv*: Vendor, Product ID, Size	-	R11 Drive failure	-	-
-	-	-	R12 CtlrN failure	-	-
-	Power fail at system in location *sysLocation*. System is running on battery.	-	U20 pwr fail, on batt	-	-
-	Power restored at system in location *sysLocation*.	-	U21 power restored	-	No action required.
-	Battery recharged to normal condition at system in location *sysLocation*.	-	-	-	-

Glossary

A

Access Control List (ACL)
A list that enumerates the rights of users or groups of users to access resources.

Agent
A program that performs one or more services. The HP NetStorage device uses backup agents to back up data remotely.

Aggregation
The combining of multiple similar or related operations into a single one.

Archive directory
Volume directory structure information on a backup tape created by the HP NetStorage 6000. This information is not directly accessible to the user. Its function is to speed up restore operations.

Archive header
General backup information found only on the first tape of a backup set.

B

Backup job
A list of volumes and backup type (full or differential) affecting the way the volumes are copied onto the tape and when the job is executed.

C

Checkpoint

A read-only copy of a volume fixed to a specified date. A checkpoint appears as a directory within a virtual volume.

CIFS

See Common Internet File System.

Collision

The result of two devices transmitting signals at the same time on the same channel, usually resulting in a garbled transmission. The HP NetStorage 6000 allows you to view collisions via the status tab.

Common Internet File System (CIFS)

A standard way of sharing resources over an IP Network. This standard supersedes SMB.

Community String

The SNMP keyword required for network management tools to retrieve operational or configuration information from the device.

Credentials

A user's account name and password.

D

Daemon

A process that is always running on a computer system (typically perpetually) to service a particular set of requests.

DHCP

See Dynamic Host Configuration Protocol.

Differential backup

A backup of only those files that have changed since the last full backup.

Domain (NT)

A group of computers whose login across the network is authenticated through the NT Server. The HP NetStorage device supports multiple domain environments by using the NT Master Domain model. The HP NetStorage device logs in to the resource domain, but authenticates users on a potentially different authentication domain. This is the Network Neighborhood domain that the HP NetStorage device appears in.

Domain (TCP/IP)

An alphanumeric representation of an association of computers. (For example, hp.com. **com** is a top level domain and **hp** is a second level domain.

Domain Name Service (DNS)

A network that translates domain names into IP addresses. If you have multiple DNS servers on your network and one DNS server cannot translate a domain name, it asks another one, and so on, until the IP address is found. The first DNS server that is queried is known as the Primary DNS, the second DNS server is known as the Secondary DNS. Each DNS server has a unique IP address.

Dynamic Host Configuration Protocol (DHCP)

Software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. It eliminates having to manually assign IP addresses, and it allows a larger group of machines to share a limited pool of addresses, assuming not all users are logged on at the same time. DHCP can assign a new address to each machine at startup (dynamic) or permanent (static) addresses can be assigned. Newer DHCP servers dynamically update the DNS servers after making assignments.

F

File Volume

File Volumes are the basic unit of logical storage for a file system on the HP NetStorage 6000. For Microsoft Windows users, the file volume is analogous to the C: drive.

Full backup

A backup of all the files in the selected file volume(s).

G

Gateway

A combination of hardware and software that links two different networks.

Gateway address

The IP address of a network server or host that functions as a gateway to other networks through communication lines or other network topologies.

Group Identification (GID)

A number in the UNIX environment that identifies a group of individuals or services to a computer system.

H

Hot spare

A previously installed physical drive used as a backup in case an assigned drive fails. The hot spare automatically takes over the duties of the failed drive. The HP NetStorage 6000 allows you to set the number of hot spares desired.

I

IP address

A unique 32-bit value that identifies network hosts using TCP/IP. An IP address, or block of addresses, is assigned upon application to organizations responsible for that function. No two network hosts can be assigned the same IP address. Each address consists of a network number, optional subnetwork number and host number, written as four numbers separated by periods. Each number can be 0 to 255.

L

Local Area Network (LAN)

A network of interconnected workstations sharing the resources of a single processor or server, typically within the area of a small office building.

Logical drive

A logical grouping of one or more physical drives on a system. In systems that employ RAID controllers, logical drives are roughly equivalent to what is commonly referred to as a RAID set.

M

Machine account

All NT workstations and servers on a network must be provided with a machine account in order to participate in a domain.

Media Access Control (MAC) address

A unique, hardware specific address used to identify a network node.

Meta-data

Data that describes data. This includes files names, file properties and security information, and lists of block addresses at which each file's data is stored.

Mount

To make a portion of a file system on a remote computer accessible to a local (client) computer. The term is most commonly used with UNIX-based computers. The analogous term using in Windows networking is Share.

N

Network File System (NFS)

An open operating system designed by Sun Microsystems that allows all network users to access shared files stored on computers of different types. Users can manipulate shared files as if they were stored locally on the user's own hard disk.

With NFS, computers connected to a network operate as clients while accessing remote files, and as servers while providing remote users access to local shared files. The NFS standards are publicly available and widely used.

NFS

See Network File System.

Network Interface Card (NIC)

An expansion card or other device used to connect a computer to a local area network.

NIS Domain

The appropriate NIS domain name that defines which Host, User and Group files are applicable for this device. A master NIS server may manage multiple file sets and the NIS domain defines which set is associated with this device.

NIS Server address

The IP address of the master server that automatically provides updates to the Host, User and Group files.

P

Packet

A block of information sent across a network. Packets contain header (which handle addressing), error correction, checksums, and data.

Permission

The ability of a particular user in a multi-user computer environment to access a particular resource by means of a user account. Permissions are stored in the system, in a file called a permissions log. Permissions are checked when a user attempts to access a resource.

Permission bits

Bits that identify the read/write/execute (rwx) privileges for a UNIX file's owner, group, and anyone else that needs access to the file (other).

Physical drive

A term for the hard drives installed in the HP NetStorage 6000. 3 to 10 physical drives may be installed in the unit. A minimum of 3 drives is required for RAID 5 configuration.

Port Aggregation

Distributing outbound server traffic between two or more NICs providing a wider data path. This is useful for servers or applications where most of the traffic flows in one direction from the server to the client. The NICs act as a team that appears as a single device with one network address.

Primary Domain Controller (PDC)

A server that has been assigned to become the primary authentication server for the Windows NT domain. It stores a copy of the Security Accounts Manager (SAM) database and uses this database to authenticate users.

R

Redundant Array of Independent Disks (RAID)

RAID is a method of combining several disk drives into a single logical storage unit. RAID offers the advantage of fault tolerance by providing real-time data recovery when a disk drive fails, increasing system uptime and network availability. RAID also increases system performance when multiple drives work together.

Relative Identification (RID) number

The relative ID for an NT user.

S

SCSI

See Small Computer System Interface.

Security Account Manager (SAM) database

A database used to authenticate users.

Server Message Block (SMB) protocol

A network protocol designed and implemented by Microsoft and used by Windows clients to communicate file access requests to Windows servers. This has been replaced by CIFS.

Share

To make a portion of a file system on a remote computer accessible to a local (client) computer. The term is most commonly used with Windows based computers. The analogous term using in UNIX networking is Mount.

Share Level Security

Security is handled by the HP NetStorage 6000. Share mode may be password-protected and may limit your access (read-only, read/write, no access) to a share. You may define the password when you create the share. The password is encrypted when transferred.

Simple Network Management Protocol (SNMP)

The protocol governing network management and the monitoring of network devices and their functions.

Simple Mail Transfer Protocol (SMTP)

A TCP/IP protocol for sending messages from one computer to another on a network. This protocol is used on the internet to route e-mail.

Small Computer System Interface (SCSI)

A SCSI interface is used to connect microcomputers to SCSI peripheral devices, such as many hard disks and printers, and to other computers and local area networks.

SMP

See Symmetric Multiprocessing.

SMTP

See Simple Mail Transfer Protocol.

SNMP

See Simple Network Management Protocol.

Subnet Mask

A 32-bit numeric mask that allows the IP address to be broken into a component that identifies the subnet on which the device resides and the ID of the device itself.

Symmetric Multiprocessing (SMP)

A computer architecture in which multiple processors share the same memory, which contains one copy of the operating system, one copy of any applications that are in use, and one copy of the data. Because the operating system divides the workload into tasks and assigns those tasks to whatever processors are free, SMP reduces transaction time.

Syslog

A file containing statistics and error messages.

System Name

The system name uniquely identifies your HP NetStorage 6000 device. You can use any combination of numbers, letters, dashes, underscores, or periods to name your device. However, the name must begin with a letter. The name you use appears on the Identity screen of the NetStorage web interface, in Network Neighborhood in a Windows networking environment, and on the HP NetStorage 6000's front panel display.

T

Tape label

General backup information available on all backup tapes created by the HP NetStorage 6000.

Tape serial number

A unique number assigned to every backup tape created by the HP NetStorage 6000.

Tape protection

The length of time a backup tape created by the HP NetStorage 6000 cannot be overwritten unless otherwise specified in the Run Now option. Tape protection is a safety device to prevent backup tapes from being overwritten prematurely.

TCP/IP

A commonly used networking protocol that allows interconnection of different network operating systems. Stands for Transmission Control Protocol/Internet Protocol.

Telnet

A protocol that provides console services remotely. The Telnet program runs on your computer and connects your PC to the NetStorage server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console.

U

Uninterruptible Power Source (UPS)

A source of electrical power that is not affected by outages in the external power source.

User Authentication

See Authentication.

User Identification (UID)

A unique number in the UNIX environment that identifies an individual to a computer system.

User Level Security

The HP NetStorage 6000 uses a domain controller to authenticate users when they access the device. Access Control Lists (ACL) define a user's access rights to a particular object.

V

Virtual volume

A volume containing checkpoints for a real volume. This allows you to view the checkpoints currently existing on the HP NetStorage 6000.

Index

A

Accessing data
- UNIX 8-1
- Windows 4-14

Alarm reset button E-1
Alerts settings
- SMTP/Email 3-7
- SNMP/Network management 3-8
- Syslog 3-9

Allowing access to data
- UNIX 8-1
- Windows 4-14

Approve file
- UNIX 4-15

ARCserveIT 11-2
Asset number 3-10
Assigning hot spare drives 4-7
Associating UNIX and NT accounts 3-14
Authentication domain name 3-6
Autoloader 5-1
- cleaning 5-1
- loading internal tapes 5-1
- loading tapes 5-1
- loading the magazine 5-1
- ordering tapes 5-1

B

Backup 5-4
- changing schedule 5-21
- creating 5-14
- job status 5-11
- local 5-5
- remote 5-6
- tape protection window 5-21

Backup and restore tab 5-1
BackupExec 11-4
Browser 1-9
Browser issues E-4

C

CA Unicenter TNG Framework 10-7
Capacity threshold 3-8
Central processing unit
- specifications C-1

Checkpoints
- backing up 5-17
- creating 5-9
- deleting 5-10
- editing 5-9
- managing 5-10
- overview 5-7
- renaming 5-10

Client activity 6-7
Computer Associates Unicenter TNG Framework 10-1
Configuration
- administrative password 3-12
- date and time 3-11
- informational settings 3-10
- SMTP/Email 3-7
- SNMP/Network Management 3-8
- system log 3-9
- UNIX 3-4
- Windows 3-6

Configuration tab 3-1
Contact phone number 3-10
Cooling fans 6-4
CPU and memory utilization 6-5
CPU specifications C-1
Creating
- backup job 5-14
- directory 4-12
- file volume 4-9
- logical drive 4-4
- mount points 8-1
- shares 4-14

Customer support
- Email 9-1
- phone 9-1
- requesting information 9-1
- URL 9-1

D

Date settings 3-11
Deleting
- directory 4-13
- file volume 4-11
- logical drive 4-5

Determining component failure E-6
Directories 4-12
- creating 4-12
- deleting 4-13
- renaming 4-12
- restoring 5-20

Disabling NIS 3-18
DNS settings 3-3
Domain Name Service 3-3
Drive specifications C-1

E

Editing
- group map file 3-20
- user map file 3-19

Editing the host access file 4-15
Email notification of hardware failure 3-7
Enabling NIS 3-18
Environmental monitoring 6-4
Environmental specifications C-3
Error codes E-10
Error notification
- email 3-7
- front panel E-10
- SNMP server 3-8
- tape log 5-14

Event log 6-3
Expanding file volumes 4-10
Exports file
- UNIX 4-15

F

File volumes 4-9
  creating 4-9
  deleting 4-11
  expanding 4-10
  renaming 4-10
  viewing information 4-8
Files
  restoring 5-20
Full Name Mapping 3-14

G

GID 8-1
Group accounts
  NIS 3-17
Group ID 8-1
Group map file
  editing 3-20

H

Hardware
  environmental
    specifications C-3
  error codes E-10
  features C-3
  performance specifications C-3
  power specifications C-3
  purchasing 9-1
  regulatory compliance C-3
  security and safety C-3
  specifications C-3
  status summary 6-1
  upgrade options C-3
Hardware settings 3-14
Help
  online 1-14
Heterogeneous environment
  security 8-9
Host access
  UNIX 4-15
Hosts file management 3-4
Hot spare 4-7
HP limited warranty statement B-6
HP Network Node Manager 10-4
HP OpenView Network Node
    Manager 10-4
HP OpenView OmniBack II 11-5
HP SureStore DLT Autoloader
    5-1
  cleaning 5-1
  loading internal tapes 5-1
  loading tapes 5-1
  loading the magazine 5-1
  ordering tapes 5-1
HP TopTools 10-3

I

Identity tab 2-1
Information report 7-1
Informational settings 3-10

L

Local backup 5-5
Log file
  NetStorage events 6-3
Logical drive
  creating 4-4
  deleting 4-5
  information 4-3
  rebuilding 4-6

M

Management applications 10-1
ManageX 10-10
Map files
  modifying 8-12
Mapping
  user name 3-14
Mapping NT and UNIX users 8-12
Mapping UNIX and NT accounts
    3-14
Mixed-mode security 8-9
Modifying
  group map file 3-20
  user map file 3-19
Modifying map files 8-12
Mount points
  creating 8-1

N

NAS 1-1
Network attached storage (NAS)
    1-1
Network Information Services
  disabling 3-18
  enabling 3-18
  group accounts 3-17
  user accounts 3-16
Network management settings 3-8
Network Node Manager 10-1
Network settings
  UNIX 3-4
  Windows 3-6
Network transmission
  information 6-6
NIS
  disabling 3-18
  enabling 3-18
  group accounts 3-17
  user accounts 3-16
NT and UNIX
  security configuration 8-12
NT to UNIX security 8-11

O

Online help 1-14
OpenView Network Node
    Manager 10-4
Operating system
  upgrading from the Web 9-4
  upgrading options 9-3
Ordering
  replacement parts C-11
  tapes 5-1
  upgrade kits C-11

Index

P

Partition a drive 4-9
Passwords 3-12
  changing 3-12
  removing 3-12
PDC 3-6
PDF-format User's Guide 1-13
Performance specifications C-3
Physical drive
  hot spare 4-7
Physical drive information 4-2
Power specifications C-3
Power supply 6-4
  attaching UPS 3-14
Primary domain controller 3-6
Printing help files 1-14
Purchasing hardware and upgrades 9-1

R

RAID set 4-3
Rebuilding
  logical drive 4-6
Redundant power supply 1-3
Registering 9-2
Regulatory compliance information C-3
Remote backup 5-6
Remote backup applications
  ARCserveIT 11-2
  BackupExec 11-4
  OmniBack II 11-5
Renaming directories 4-12
Renaming file volumes 4-10
Replacement parts C-11
Report tab 7-1
Reporting 7-1
Resizing file volumes 4-10
Resource domain name 3-6
Restore
  files and directories 5-20
  job status 5-12
  overview 5-18
  volumes 5-18

S

Security 8-1
  managing in a heterogeneous environment 8-9
  mixed mode 8-9
  share level 8-4
  user level 8-4
Security and safety information C-3
Settings and features 5-21
Share level security
  Windows 8-4
Share-level security 8-4
Shares
  creating 4-14
Simple Mail Transfer Protocol 3-7
Simple Network Management Protocol 3-8
SMTP 3-7
SNMP 3-8
Software license agreement A-2
Spare drive
  hot swappable 4-7
Statements A-1
Status lights E-6
Status summary 6-1
Status tab 6-1
Storage tab 4-1
Support 9-1
Support tab 9-1
Swap hard drive 4-7
System location 3-10
System log 3-9
System messages 6-3
System name 3-3
System settings
  administrative password 3-12
  date and time 3-11
  informational 3-10

T

Tape backup job status 5-11
Tape log 5-14
Tape magazine 5-13
Tape protection window 5-21
Tape restore job status 5-12
Tapes
  cleaning 5-1
  formatting 5-4
  information 5-14
  loading 5-1
  ordering 5-1
Telnet 1-3
Temperature 6-4
Time settings 3-11
Top Tools 10-3
Traps 3-8
Troubleshooting
  browser issues E-4
  component failure E-6
  general issues E-1
  UPS E-8
Trusted hosts file management 3-4

U

UID 8-1
Unicenter TNG Framework 10-7
Uninterruptible power supply 3-14, C-1
UNIX
  creating mount points 8-1
  security 8-1
  security configuration 3-4
  settings 3-4
UNIX and NT
  security configuration 8-12
UNIX approve file 4-15
UNIX exports file 4-15
UNIX file management
  password 3-12
  trusted hosts 3-4
UNIX host access 4-15
UNIX to NT security 8-10

Upgrade
kits C-11
options (hardware) C-3
purchasing 9-1
Upgrading
adding hard drives 4-2
Upgrading your operating system
checking for upgrades 9-3
file already downloaded 9-5
from the web 9-4
options 9-3
UPS 3-14
specifications C-1
troubleshooting E-8
user accounts
NIS 3-16
User ID 8-1
User level security
Windows 8-4
User map file
editing 3-19
User name mapping 3-14
Using help 1-14

V

Viewing
client activity 6-7
CPU utilization 6-5
file volume information 4-8
logical drive information 4-3
network transmisson information 6-6
physical drive information 4-2
system messages 6-3
Volume capacity threshold 3-8
Volumes
creating 4-9
deleting 4-11
expanding 4-10
renaming 4-10
restoring 5-18
view information 4-8

W

Warranty support B-3
Web interface 1-9
Windows
creating shares 4-14
security configuration 3-6
settings 3-6
Windows share level security 8-4
Windows to UNIX mapping 8-12
Windows user level security 8-4
WINS servers 3-6
Write-protecting tapes 5-18